NOTICE TO THE UNITED STATES JUDICIAL PANEL ON MULTIDISTRICT LITIGATION OF MULTICIRCUIT PETITIONS FOR REVIEW

IN RE: Federal Communications Commission, *Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program*, Report and Order, Order, and Further Notice of Proposed Rulemaking (released November 25, 2022; published in the Federal Register on February 6, 2023)	No. __-____

NOTICE OF MULTICIRCUIT PETITIONS FOR REVIEW

Pursuant to 28 U.S.C. § 2112(a)(3) and the Rules of Procedure of the United States Judicial Panel on Multidistrict Litigation, the Federal Communications Commission hereby provides notice of two petitions for review, filed in two different courts of appeals, of the same final agency action. *See Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program*, Report and Order, Order, and Further Notice of Proposed Rulemaking, (released November 25, 2022), 88 Fed. Reg. 7592 (February 6, 2013).

Each petition for review was filed within ten days after the challenged order's publication in the Federal Register and received by the FCC from the petitioners within that ten-day period. As required by Panel Rule 25.2, we submit with this notice: (1) a schedule (Attachment A) listing the petitions for review; (2) copies of each petition (Attachment B); and (3) the order the petitioners are challenging (Attachment C). In accordance with Panel Rule 25.3, as indicated in the attached certificate of service, the FCC is serving this notice on the clerks of the courts where the petitions for review have been filed as well as on counsel for all parties in the petitions for review.

Dated: February 27, 2023

Respectfully submitted,

/s/ Matthew J. Dunne

P. Michele Ellison
General Counsel

Jacob M. Lewis
Deputy General Counsel

Sarah E. Citrin
Assistant Deputy General Counsel

Matthew J. Dunne
Counsel

FEDERAL COMMUNICATIONS COMMISSION
45 L Street NE
Washington, DC 20554
(202) 418-1740
fcclitigation@fcc.gov
matthew.dunne@fcc.gov

SCHEDULE REQUIRED BY RULE 25.2 OF THE RULES OF PROCEDURE OF THE UNITED STATES JUDICIAL PANEL ON MULTIDISTRICT LITIGATION

Date of Federal Register publication of order: February 6, 2023

Case Name	Circuit Court	Docket Number	Filing Date	Date received by FCC
Hikvision USA, Inc. v Federal Communications Commission and United States of America	D.C. Circuit	23-1032	February 13, 2023	February 14, 2023
Dahua Technology USA Inc. v Federal Communications Commission and United States of America	Ninth Circuit	23-206	February 14, 2023	February 14, 2023

Matthew J. Dunne
Federal Communications Commission
Washington, DC 20554
(202) 418-1740
matthew.dunne@fcc.gov
fcclitigation@fcc.gov

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

HIKVISION USA, INC. *Petitioner*, v. FEDERAL COMMUNICATIONS COMMISSION and UNITED STATES OF AMERICA, *Respondents*.	Case No. 23-1032

PETITION FOR REVIEW

Pursuant to 28 U.S.C. §§ 2342(1) and 2344, 47 U.S.C. § 402(a), 5 U.S.C. § 706, and Rule 15(a) of the Federal Rules of Appellate Procedure, Hikvision USA, Inc. ("Hikvision") hereby petitions this Court for review of the decision of the Federal Communications Commission (the "FCC" or the "Commission") adopted as FCC 22-84 on November 11, 2022 and released on November 25, 2022, titled *Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program*, *Protecting Against National Security Threats to the Communications Supply Chain Through the Competitive Bidding Program*, Report and Order, Order, and Further Notice of Proposed Rulemaking, ET Docket No 21-232, EA Docket No. 21-233 (rel. Nov. 25, 2022) (the "*Order*").

On February 6, 2023, the *Order* was published in the Federal Register at 88 Fed. Reg.7592. A copy of the *Order* is attached as Exhibit A to this Petition. Venue in this Court is proper under 28 U.S.C. § 2343.

Hikvision was a participant in the proceeding below and is aggrieved by the challenged *Order*. Hikvision seeks review on the grounds that the *Order* exceeds the FCC's jurisdiction and its statutory authority; violates the Equal Protection and Bill of Attainder Clauses of the United States Constitution; violates the Communications Act and the Administrative Procedure Act; and is arbitrary and capricious, an abuse of discretion, not supported by substantial evidence, and otherwise contrary to law.

Hikvision respectfully requests that the Court hold unlawful, vacate, enjoin, and set aside the *Order* and grant such further relief as may be appropriate.

February 13, 2023

Respectfully submitted,

/s/ *Timothy J. Simeone*

John T. Nakahata
Christopher J. Wright
Timothy J. Simeone
John R. Grimm
Deepika Ravi
HWG, LLP
1919 M St., N.W., 8th Floor
Washington, D.C. 20036
(202) 730-1300
tsimeone@hwglaw.com

Counsel to Hikvision USA, Inc.

CERTIFICATE OF SERVICE

I hereby certify that, on February 13, 2023, the foregoing was served by U.S. mail upon the following parties:

Merrick Garland
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530

P. Michele Ellison
General Counsel
Federal Communications Commission
445 12th Street SW, 8th Floor
Washington, DC 20554

Respectfully submitted,

/s/ *Timothy J. Simeone*
Timothy J. Simeone

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

HIKVISION USA, INC. *Petitioner*, v. FEDERAL COMMUNICATIONS COMMISSION and UNITED STATES OF AMERICA, *Respondents*.	Case No. 23-1032

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1 and Circuit Rule 26.1, Petitioner Hikvision USA, Inc. ("Hikvision USA") states the following.

Hikvision USA is a California corporation and wholly owned subsidiary of Hangzhou Hikvision Digital Technology Company, Limited, which is publicly traded on China's Shenzhen Stock Exchange. Hikvision USA sells security equipment, primarily surveillance cameras and related devices, through a network of distributors—mostly small-to medium-sized businesses—that over the past ten years has included approximately 50,000 independently owned and operated dealers across the United States.

As a publicly traded company, Hikvision USA's parent company, Hangzhou Hikvision Digital Technology Co., Ltd., has a diverse set of public and private shareholders. The largest shareholder, owning approximately 36.08% of the company, is China Electronics Technology HIK Group Co., Ltd., an indirectly state-owned enterprise of the People's Republic of China, and the second largest shareholder—with 10.20% of Hangzhou Hikvision Digital Technology Co., Ltd—is founder, Hong Kong resident Kung Hung Ka (also written Gong Hongjia). No other person or entity holds more than 10% of the shares of Hangzhou Hikvision Digital Technology Co., Ltd.

Other than Hangzhou Hikvision Digital Technology Company, no other person or entity holds a 10% or greater ownership interest in Hikvision USA.

February 13, 2023

Respectfully submitted,

/s/ *Timothy J. Simeone*

John T. Nakahata
Christopher J. Wright
Timothy J. Simeone
John R. Grimm
Deepika Ravi
HWG LLP
1919 M St., N.W., 8th Floor
Washington, D.C. 20036
(202) 730-1300
tsimeone@hwglaw.com

Counsel to Hikvision USA, Inc.

CERTIFICATE OF SERVICE

I hereby certify that, on February 13, 2023, the foregoing was served by U.S. mail upon the following parties:

Merrick Garland
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530

P. Michele Ellison
General Counsel
Federal Communications Commission
445 12th Street SW, 8th Floor
Washington, DC 20554

Respectfully submitted,

/s/ *Timothy J. Simeone*
Timothy J. Simeone

No. _____

In the United States Court of Appeals
FOR THE NINTH CIRCUIT

Dahua Technology USA Inc.,

Petitioner,

v.

Federal Communications Commission and
United States of America,

Respondents.

On Petition for Review
from the Federal Communications Commission

PETITION FOR REVIEW

MORGAN, LEWIS & BOCKIUS LLP
Andrew D. Lipman
Russell M. Blau
1111 Pennsylvania Avenue, NW
Washington, DC 20004
T: (202) 739-3000
F: (202) 739-3001

Counsel for Petitioner Dahua Technology USA Inc.

PETITION FOR REVIEW

Pursuant to 5 U.S.C. § 706, 47 U.S.C. § 402(a), 28 U.S.C. §§ 2342(1) and 2344, and Federal Rule of Appellate Procedure 15(a), Petitioner Dahua Technology USA Inc. ("Dahua") hereby petitions this Court to review the Federal Communications Commission's Report and Order adopted on November 11, 2022 and released November 25, 2022, in the proceedings captioned *In the Matter of Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*, ET Docket No. 21-232 and *In the Matter of Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program*, EA Docket No. 21-233, FCC 22-84 (the "Order"). A copy of the Order is attached as Exhibit A to this petition.

Venue is proper in this Court pursuant to 28 U.S.C. § 2343.

Dahua petitions this Court to set aside the Order pursuant to 5 U.S.C. § 706(2) because it is arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law; contrary to constitutional right, power, privilege, or immunity; in excess of statutory jurisdiction, authority, or limitations, or short of statutory right; and without observance of procedure required by law.

Accordingly, Dahua respectfully requests that this Court hold unlawful, vacate, and set aside the Order, and that it provide such additional relief as may be appropriate.

Dated: February 14, 2023

Respectfully submitted,

/s/ Russell M. Blau
MORGAN, LEWIS & BOCKIUS LLP
Andrew D. Lipman
Russell M. Blau
1111 Pennsylvania Avenue, NW
Washington, DC 20004
T: (202) 739-3000
F: (202) 739-3001
andrew.lipman@morganlewis.com
russell.blau@morganlewis.com

Counsel for Dahua Technology USA Inc.

CERTIFICATE REGARDING SERVICE

In accordance with Fed. R. App. P. 15(c), I certify that the names of the Respondent and the addresses where they may be served with copies of this Petition are as follows:

Federal Communications Commission
c/o P. Michele Ellison, Acting General Counsel, Office of General Counsel
45 L Street NE
Washington, DC 20554

Merrick B. Garland
Attorney General of the United States
c/o U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

Dated: February 14, 2023

/s/Russell M. Blau

PETITIONER'S RULE 26.1 CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1(a), Dahua Technology USA Inc. states that it is a wholly-owned subsidiary of Zhejiang Dahua Technology Co., Ltd., a privately owned corporation incorporated in China. Dahua Technology USA Inc.'s only direct parent company is Dahua Technology (HK) Ltd., a Hong Kong incorporated entity with its principal office at 13/F Gloucester Tower, The Landmark, 15 Queen's Road Central, Central, Hong Kong. Dahua Technology (HK) Ltd. is a wholly-owned subsidiary of Zhejiang Dahua Technology Co., Ltd.

Dated: February 14, 2023

/s/ Russell M. Blau

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program	)	ET Docket No. 21-232
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program	)	EA Docket No. 21-233

REPORT AND ORDER, ORDER, AND FURTHER NOTICE OF PROPOSED RULEMAKING

Adopted: November 11, 2022 **Released: November 25, 2022**

Comment Date: 30 days after Federal Register publication
Reply Comment Date: 60 days after Federal Register publication

By the Commission: Chairwoman Rosenworcel and Commissioners Carr, Starks, and Simington issuing separate statements.

TABLE OF CONTENTS

I. INTRODUCTION

1. Today, we build upon the important ongoing efforts by the Commission, Congress, and the Executive Branch to take further action to protect the security of America's critical communications networks and equipment supply chains. In this Report and Order (ET Docket 21-232), we amend our rules related to equipment authorization to further secure our communications networks and supply chains from equipment that poses an unacceptable risk to national security of the United States or the security and safety of United States persons. Specifically, as proposed in the *Notice of Proposed Rulemaking*

(*NPRM*),[1] we adopt revisions to our equipment authorization program to prohibit authorization of equipment that has been identified on the Commission's Covered List – published pursuant the Secure and Trusted Communications Networks Act of 2019[2] – as posing an unacceptable risk to national security of the United States or the security or safety of United States persons, and we prohibit the marketing and importation of such equipment in the United States. We also address what constitutes "covered" equipment for purposes of implementing the equipment authorization prohibition that we are adopting. The actions we take today in adopting new rules and procedures comply with Congress's directive in the Secure Equipment Act of 2021[3] to prohibit authorization of "covered" equipment on the Covered List within one year of that Act's enactment and lay the foundation to prohibit the authorization of any additional "covered" equipment that may be added to the Covered List based on a determination that such equipment poses an unacceptable risk to national security.

2. We also adopt a Further Notice of Proposed Rulemaking on issues raised in the *Notice of Proposed Rulemaking*. First, we seek further comment on potential additional revisions to the rules and procedures associated with prohibiting the authorization of "covered" equipment in our equipment authorization program. Second, we seek additional comment on proposed revisions to the Commission's competitive bidding program (EA Docket No. 21-233). We do not address, at this time, the cybersecurity-related issues raised in the *Notice of Inquiry*.[4]

3. *Executive summary.* In adopting the Commission's proposal to prohibit authorization of any communications equipment that has been placed on the Covered List, this Report and Order –

- Places the Commission's actions in this proceeding within the context of several ongoing efforts by the Commission, Congress, and the Executive Branch to protect the security of the United States communications networks and equipment supply chains;
- Finds that the Commission has the requisite statutory authority to implement this prohibition in its equipment authorization program, as further affirmed by the Secure Equipment Act of 2021;
- Adopts several revisions to the Commission's part 2 rules concerning equipment authorization processes, including authorization under either the equipment certification procedures (which involve use of Telecommunication Certification Bodies) or the Supplier's Declaration of Conformity (SDoC) procedures --
    - Requires all applicants for equipment certification to attest in their applications (in the form of a written and signed certification) that the particular equipment for which they seek certification is not "covered" equipment (i.e., is not communications equipment that has been identified and placed on the Commission's Covered List);

[1] *Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program*, EA Docket No. 21-233, Notice of Proposed Rulemaking and Notice of Inquiry, 36 FCC Rcd 10578 (2021) (*NPRM* and *NOI*, respectively).

[2] Pursuant to sections 2(a) and (d) of the Secure and Trusted Communications Networks Act of 2019, and sections 1.50002 and 1.50003 of the Commission's rules, the Federal Communications Commission's Public Safety and Homeland Security Bureau (PSHSB) publishes a list of communications equipment and services that have been determined by one of the sources specified in that statute to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons ("covered" equipment). Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601-1609 (Secure Networks Act); 47 CFR §§ 1.50002, 1.50003.

[3] Secure Equipment Act of 2021, Pub. L. No. 117-55, 135 Stat. 423 (2021) (codified at 47 U.S.C. § 1601 (Statutory Notes and Related Subsidiaries)) (Secure Equipment Act).

[4] *NOI*, 36 FCC Rcd at 10615-18, paras. 98-105. In the *NOI*, the Commission sought broad comment on other possible actions the Commission could take to create incentives in equipment authorization processes for improved trust through the adoption of cybersecurity best practices in consumer devices. *Id.*

- Prohibits any entity that has been identified on the Covered List as producing "covered" equipment from obtaining equipment authorization through the Commission's SDoC procedures, requiring such entities instead to use the certification procedures;
- No longer exempts any "covered" equipment from the need for an equipment authorization, and requires that any entity identified on the Covered List as producing "covered" equipment to obtain an equipment certification;
- Requires the each applicant for equipment certification designate a U.S. agent for services of process (regardless of whether the applicant is domestic or foreign);
- With respect to potential revocation of equipment authorizations, (1) establishes streamlined procedures for revoking authorizations granted after adoption of the prohibition on authorization of "covered" equipment if the application has included false statement or representation relating to "covered" equipment and (2) concludes that the Commission has authority to revoke, in the future, authorizations of "covered" equipment that had been authorized prior to adoption of this Report and Order;
- Discusses implementation of the prohibition with respect to equipment on the current Covered List produced by certain entities:
  - Prohibits authorization of all telecommunications and video surveillance equipment produced by Huawei and ZTE (and that of their subsidiaries and affiliates);
  - Prohibits authorization of telecommunications equipment and video surveillance equipment produced by Hytera, Hikvision, and Dahua (and their respective subsidiaries or affiliates) until such time as the Commission approves these entities' plans and measures that will to ensure the such equipment will not be marketed and sold to for "the purpose of public safety, security of government facilities, physical surveillance of critical infrastructure, or other national security purpose";
- Requires entities named on the Covered List as producing "covered" equipment to provide the Commission information on other entities (such as their subsidiaries and affiliates) also identified on the Covered List but are not specifically named; and
- Addresses various other issues raised in the proceeding (e.g., the cost effectiveness of the rules, challenges on constitutional grounds, consistency with trade obligations, enforcement).

- The Order adopts an interim freeze on further processing or grant of equipment authorization applications for equipment that is produced by any entity identified on the Covered List as producing "covered" equipment, effective until the rules prohibiting such authorization become effective.
- In the Further Notice of Proposed Rulemaking, the Commission seeks comment on further revisions to the equipment authorization program and competitive bidding program.
  - *Equipment Authorization Program* – seeks further comment on:
    - the extent to which component parts should be considered in the Commission's prohibition on authorization of "covered" equipment;
    - the extent to which the Commission should revoke any previously authorized equipment that is "covered" equipment (and if so, based on which considerations and procedures); and
    - whether to require all applicants seeking equipment certification to have a U.S.-based responsible party to help ensure compliance with the Commission's equipment authorization program rules.
  - *Competitive Bidding Program* – seeks further comment on possible revisions to the competitive bidding rules to address national security concerns.

II. BACKGROUND

4. In the *Notice of Proposed Rulemaking* and *Notice of Inquiry* (*NPRM* and *NOI*), the Commission proposed to revise its rules and procedures relating both to its equipment authorization program and its competitive bidding program to leverage the processes associated with these programs to help keep untrusted equipment and vendors out of U.S. networks.[5] As the Commission made clear, the efforts underway in the instant proceedings are intended to be among the additional steps that the Commission is taking to be consistent with, and build upon, other efforts underway at the Commission, Congress, and the Executive Branch to protect our nation's supply chain from equipment and services that pose a national security risk or a threat to the safety of U.S. persons.[6]

A. Ongoing Congressional, Commission, and Executive Branch Efforts

5. The instant proceedings were initiated shortly after the Commission's first publication, on March 12, 2021, of its Covered List concerning communications equipment and services that have been determined to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons.[7] The Commission maintains this list pursuant to the Secure and Trusted Communications Networks Act of 2019 (Secure Networks Act), which was enacted one year earlier on March 12, 2020.[8] In the *NPRM*, the Commission specifically proposed prohibiting the authorization of any "covered" equipment on the Covered List.[9]

6. As discussed below, the Secure Networks Act is only one of many Congressional, Commission, and Executive Branch actions that inform these proceedings. At an increasingly rapid pace in recent years, the United States government has moved to protect the security of the communications networks across the country. Congress, the Executive Branch, and the Commission have prioritized the importance of identifying and eliminating potential security vulnerabilities in communications networks and their supply chains.[10] Also, subsequent to adoption of the *NPRM and NOI* in June of 2021, Congress enacted the Secure Equipment Act of 2021, which further informs the Commission's efforts to prohibit the authorization of "covered" equipment in the rules and procedures associated with the Commission's equipment authorization program.

7. *Congressional and Executive Branch actions.* In recent years, Congress and the Executive Branch have taken several steps to promote more secure networks and supply chains. We mention some of those efforts here. As discussed in the *NPRM,* in December 2017 Congress enacted the National Defense Authorization Act for Fiscal Year 2018 (2018 NDAA), which included provisions that addressed continuing concerns over the purchase and use of certain communications equipment, specifically barring the Department of Defense from using telecommunications equipment or services produced or provided by Huawei Technologies Company (Huawei) or ZTE Corporation (ZTE).[11]

8. In the following year, in August 2018, Congress enacted section 889 of the National Defense Authorization Act for Fiscal Year 2019 (2019 NDAA), in which it expanded the prohibitions that the federal government must implement regarding the use not only of Huawei and ZTE equipment but the use of certain equipment produced by three additional companies.[12] Pursuant to section 889(a), the 2019

[5] *See NPRM* and *NOI*, 36 FCC Rcd 10578.

[6] *See generally id.* at 10580-89, paras. 6-22 (detailing the recent Commission, Congressional, and Executive Branch actions to protect the security of the nation's communications systems).

[7] *Id.* at 10579, 10589, paras. 3, 22.

[8] *Id.*at 10579, 10585, 10589, paras. 3, 15, 22.

[9] *Id.*at 10579, 10596-10606, paras. 3, 40-64.

[10] *See id.* at 10580, 10580-10589, paras. 6 & n.4, 7-22.

[11] *See* Pub. L. 115-91, 131 Stat. 1283, 1762, § 1656.

[12] *See* Pub. L. 115-232, 132 Stat. 1636.

NDAA prohibited the head of an Executive Branch agency from using federal funds to procure or obtain equipment, services, or systems that use "covered telecommunications equipment or services" as a "substantial or essential component of any system, or as critical technology as part of any system" after one year following the Act's enactment, and prohibited entering into contracts with an entity that uses any equipment, system, or service that uses such equipment or services after two years of enactment;[13] in section 889(f)(3), Congress defined "covered telecommunications equipment or services" as including "telecommunications equipment" produced by Huawei or ZTE (or their subsidiaries or affiliates), "video surveillance and telecommunications equipment" produced by Hytera Communications Corporation (Hytera), Hangzhou Hikvision Digital Technology Company (Hikvision), or Dahua Technology Company (Dahua) (or their subsidiaries or affiliates), or "telecommunications or video surveillance services provided by such entities or using such equipment."[14]

9. In December 2018, Congress enacted the SECURE Technology Act to create the Federal Acquisition Security Council (FASC), which includes seven Executive Branch agencies – including representatives from the Office of Management and Budget (which also chairs the Council), the General Services Administration (GSA), Department of Homeland Security (DHS), the Office of the Director of National Intelligence (ODNI), the Department of Justice (DoJ), the Department of Defense (DoD), and the Department of Commerce (DoC).[15] The Council is charged with developing a government-wide strategy to address communications supply chain risks and may recommend that other agencies remove unsecure communications services or equipment.[16]

10. In May 2019, the White House issued Executive Order 13873 on "Securing the Information and Communications Technology and Services Supply Chain." The EO declared a national emergency with respect to the security, integrity, and reliability of information and communications technology and services, and granting the Secretary of Commerce the authority to prohibit transactions of information and communications technology or services when, among other things, the transaction would pose undue risks to U.S. critical infrastructure or national security.[17] Pursuant to this EO, the Cybersecurity & Infrastructure Security Agency (CISA) established its supply chain risk management (SCRM) Task Force to work with industry and government partners to assess the national security risks stemming from vulnerabilities in information and communications technology (ICT) hardware, software and services.[18] In November 2019, the Department of Commerce began a rulemaking to implement EO 13873.[19] On January 19, 2021, the Department of Commerce published an interim final rule that sets out procedures by which the Secretary of Commerce, in consultation with the appropriate heads of other

[13] 2019 NDAA, § 889(a)-(b)(1).

[14] *Id.*, § 889(f)(3)(A)-(C). With respect to equipment produced by Hytera, Hikvision, and Dahua, and their subsidiaries and affiliates, their equipment is "covered" for certain specified purposes. *Id.* § 889(f)(3)(B).

[15] *See* P.L. 115-390, 132 Stat. 5173, 5179, §§ 1322(b)-(c).

[16] *See id*. Specifically, the FASC is responsible for establishing procedures to (1) facilitate the exclusion of entities and covered services and equipment from agency procurements, and (2) enable the removal of such services and equipment from agency information systems when it determines that those items or the parties providing them present a supply chain risk. *See* P.L. 115-390, 132 Stat. 5173, 5181, § 1323(c)(1).

[17] *See* Exec. Order No. 13873, 84 Fed. Reg. 11578 ("Executive Order on Securing the Information and Communications Technology and Services Supply Chain") (May 15, 2019), https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain (Executive Order 13873). On May 14, 2020, the President issued an order extending the emergency declaration for another year. *See* Continuation of the National Emergency with Respect to Securing the Information and Communications Technology and Services Supply Chain, 85 Fed. Reg. 29321 (May 14, 2020).

[18] https://www.cisa.gov/eo13873.

[19] U.S. Department of Commerce, Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 65316 (Nov. 27, 2019).

administrative agencies, reviews Information and Communications Technology and Services transactions to determine whether they present an undue or unacceptable risk to national security.[20]

11. In March 2020, Congress enacted the Secure 5G and Beyond Act of 2020, which requires the President to develop a strategy to ensure the security of next generation mobile telecommunications systems and infrastructure in the United States and to assist allies and strategic partners in maximizing the security of such next generation systems and infrastructure.[21] On January 19, 2021, the Department of Commerce published a National Strategy to Secure 5G Implementation Plan, which notes the involvement of Federal Departments, agencies, and other Federal agencies (including the Commission) in participating in the implementation of this plan.[22]

12. On May 12, 2021, the President issued Executive Order 14028 on "Improving the Nation's Cybersecurity," directing multiple federal agencies to promote the nation's cybersecurity and protect federal government networks, including through removing barriers to threat information sharing between government and the private sector, implementing stronger cybersecurity standards in the Federal government, and improving the software supply chain.[23] On September 15, 2022, the President issued Executive Order 14083 directing the Committee on Foreign Investment in the United States (CFIUS) to consider specific risks when reviewing covered transactions.[24] EO 14083 defines five new national security factors and elaborates on existing statutory factors when reviewing covered transactions: (1) U.S. supply chain resiliency; (2) U.S. technological leadership; (3) aggregate investment trends; (4) cybersecurity; and (5) sensitive personal data. The EO emphasizes the risks presented by foreign adversaries' access to data of U.S. persons.[25]

13. *Executive Branch actions implementing section 889 of the 2019 NDAA and other relevant federal agency actions*. Since the 2018 enactment of section 889 of the 2019 NDAA, the Federal Acquisition Regulations (FAR) System, which publishes uniform policies and procedures for acquisition by all executive agencies, has provided guidance on implementation of section 889's prohibition (per section 889(a)(1)) on the federal government with regard to procuring, obtaining, or extending a contract

---

[20] U.S. Department of Commerce, Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4909 (Jan. 19, 2021). On June 9, 2021, the White House issued Executive Order 14034, which builds upon the measures outlined in Executive Order 13873 by directing the federal government to evaluate the risks of "certain connected software applications designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary." https://www.federalregister.gov/documents/2021/06/11/2021-12506/protecting-americans-sensitive-data-from-foreign-adversaries. In November 2021, the Department of Commerce published a Proposed Rule that would implement Executive Order 14034 by providing for additional criteria that the Secretary of Commerce may consider when determining whether information and communications technology and services transactions that involve connected software applications present an undue or unacceptable risk to national security. https://www.federalregister.gov/documents/2021/11/26/2021-25329/securing-the-information-and-communications-technology-and-services-supply-chain-connected-software.

[21] *See* P.L. 116-129, 134 Stat. 223.

[22] https://www.ntia.gov/files/ntia/publications/2021-1-12_115445_national_strategy_to_secure_5g_implementation_plan_and_annexes_a_f_final.pdf

[23] Exec. Order No. 14028, 86 FR 26633 ("Improving the Nation's Cybersecurity") (May 12, 2021), https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity. These initiatives include developing guidance on critical software and identifying Internet of Things (IoT) criteria for a consumer labeling program.

[24] Exec. Order No. 14083, 87 FR 57369 ("Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States") (Sept. 15, 2022), https://www.govinfo.gov/content/pkg/FR-2022-09-20/pdf/2022-20450.pdf.

[25] *See* https://www.whitehouse.gov/briefing-room/presidential-actions/2022/09/15/executive-order-on-ensuring-robust-consideration-of-evolving-national-security-risks-by-the-committee-on-foreign-investment-in-the-united-states/.

to procure or obtain any equipment, system, or service that uses "covered telecommunications equipment or service," and the agencies' contractual prohibition (per section 889(a)(2)) as that equipment is defined in section 889(f)(3), if that equipment is a "substantial or essential component of any system, or as critical technology as part of any system."[26] Interim FAR rules were issued in 2019 and 2020 regarding the procurement and contracting prohibitions, and require that in offering equipment for procurement by a federal agency, the offeror/contractor must include representations regarding "covered" equipment defined under section 889(f)(3), which per that provision includes both "telecommunications equipment" and "video surveillance equipment."[27] In August 2020, the GSA Supply Chain Risk Management (SCRM) Review Board[28] also provided some guidance criteria for evaluating the applicability of the procurement prohibition.[29]

14. *Secure and Trusted Communications Networks Act of 2019 (Secure Networks Act)*.[30] In March 2020, the Secure Networks Act was enacted. These provisions include: requiring (pursuant to section 2(a)) that the Commission publish, and periodically update, a list of "covered communications equipment and services" that have been determined to pose national security risks,[31] requiring (per section 2(b)) that the Commission place on that list the equipment or services that are produced or provided by entities and meets certain capabilities,[32] and further requiring (per section 2(c)) that the equipment or services placed on the list be "based solely on" determinations made by four enumerated sources. In particular, these determinations and sources are limited to – (1) a "specific determination made by any executive branch interagency body with appropriate national security expertise, including the Federal Acquisition Security Council …;" (2) a "specific determination made by the Department of Commerce pursuant Executive Order No. 13873 … relating to securing the information and communications technology and services supply chain;" (3) the "communications equipment or service being covered

[26] 2019 NDAA § 889(a), (f)(3). As discussed above, section 889(f)(3) defines "covered telecommunications equipment or services" as including telecommunications and video surveillance equipment produced by Huawei, ZTE, Hytera, Hikvision, and Dahua.

[27] In 2019 and 2020, interim rules were adopted by Department of Defense, GSA, and NASA to amend the Federal Acquisition Regulation (FAR) to implement section 889(a)(1)(A) and (B) regarding the prohibition on procurement of certain covered equipment or contracting associated with covered equipment, as that equipment is defined in section 889(f)(3) of the 2019 NDAA. *See* https://www.federalregister.gov/documents/2019/12/13/2019-26579/federal-acquisition-regulation-prohibition-on-contracting-for-certain-telecommunications-and-video; https://www.federalregister.gov/documents/2020/08/27/2020-18772/federal-acquisition-regulation-prohibition-on-contracting-with-entities-using-certain. Under the FAR interim rules, implementation of these prohibitions require that an offeror of equipment or service either (1) represent, on an offer-by-offer basis, if it will or will not provide any "covered telecommunications equipment or services" (which under section 889(f)(3) includes both "video surveillance and telecommunications equipment" of named entities) to the Government, or (2) make an annual representation that it "does not" offer any equipment or service from any entity providing equipment or services listed in the definition of "covered telecommunications equipment or services," including any known subsidiaries or affiliates. *See generally id.*

[28] GSA's Office of the Chief Information Security Officer (OCISO), through its Cyber Supply Chain Risk Management (C-SCRM) Program, was established to provide a C-SCRM capability. The SCRM Review Board is responsible for handling supply chain events reported by contracting officers, including prohibited vendor disclosures. *See* IT Security Procedural Guide: OCISO Cyber Supply Chain Risk Management (C-SCRM) Program CIO-IT Security-21-117, GSA IT, Initial Release, July 11, 2022, at Introduction (p. 2).

[29] *See, e.g.*, "SCRM Criteria for Section 889 Part A" and "SCRM Criteria for Section 889 Part B," respectively, found at https://www.gsa.gov/cdnstatic/SCRM%20review%20board%20889%20PART%20A%20Rubric_0.pdf; https://www.acquisition.gov/FAR-Case-2019-009/889_Part_B.

[30] Secure Networks Act.

[31] *Id.*§ 2(a).

[32] *Id.*§ 2(b).

telecommunications equipment or services, as defined in section 889(f)(3) of [the 2019 NDAA];" or (4) a "specific determination made by an appropriate national security agency."[33]

15. The Secure Networks Act also adopted other provisions. These included requiring the Commission to: prohibit any Federal subsidy made available through a program administered by the Commission that provides funds used for the capital expenditures necessary for the provision of advanced communications service to purchase or otherwise obtain or maintain "covered" communications equipment or services (section 3); establish the Secure Networks Act Reimbursement Program to make reimbursements to certain advanced communications service providers to facilitate the removal, replacement, and disposal of certain "covered" communications equipment and services (section 4); and require each provider of advanced communications service to submit annual reports to the Commission regarding whether it has purchased, rented, leased, or otherwise obtained and "covered" communications equipment or services on or after August 14, 2018 or 60 days after new covered equipment and services are subsequently added to the Covered List (section 5).[34]

16. *Commission actions.* As discussed in the *NPRM*, the Commission has undertaken numerous efforts to address concerns about untrusted equipment (as well as services) in our nation's networks and supply chains. These include actions taken before enactment of the Secure Networks Act as well as subsequent actions, including the incorporation of specific requirements associated with the Secure Networks Act into the Commission's part 1 rules ("Secure and Trusted Communications Networks"), sections 1.50000 *et seq.*[35]

17. In November 2019, the Commission adopted the *Supply Chain Report and Order, Further Notice, and Order*, in which it adopted a rule prohibiting the use of "universal service support . . . to purchase or obtain any equipment or services produced or provided by a "covered company" that posed a national security threat to the integrity of communications networks or the communications supply chain."[36] The Commission also initially designated two Chinese companies, Huawei and ZTE, and their subsidiaries, parents, or affiliates, as "covered companies" that pose such a national security threat.[37] Although this rule was adopted pursuant to the public interest authority established in section 201(b) and

---

[33] *Id.*§ 2(a)-(c). The Secure Networks Act defines "executive branch interagency body" to mean an interagency body established in the executive branch, and "appropriate national security agency" as meaning the Department of Homeland Security, the Department of Defense, the Office of the Director of National Intelligence, the National Security Agency, and the Federal Bureau of Investigation. Secure Networks Act, §§9(7) and (9)(1), respectively. In interpreting "executive branch interagency body with appropriate national security expertise" under § 2(c)(1) of the Secure Networks Act, the Commission found that it has no discretion to ignore determinations from Team Telecom/the Committee and the Committee on Foreign Investment in the United States. These two interagency bodies routinely provide expertise to the Commission on national security questions. *Supply Chain 2nd R&O*, 35 FCC Rcd at 14312-13, paras. 61-62.

[34] Secure Networks Act §§ 3, 4, and 5. Section 7 tasks the Commission with enforcing the Secure Networks Act and adds penalties beyond those in the Communications Act and our rules for violations of section 4. *See id.* § 7. Section 9 sets forth definitions of certain terms in the Secure Networks Act, including "advanced communications service" and "communications equipment or service." *See id.* § 9.

[35] *NPRM*, 36 FCC Rcd at 10582-83, 10585-87, paras. 10-11, 14-18.

[36] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd 11423, 11433, para. 26 (2019) (*Supply Chain Order*).). The Fifth Circuit upheld this rule against a challenge by Huawei, concluding that "[a]ssessing security risks to telecom networks falls in the FCC's wheelhouse," and that the Commission "reasonably acted within the broad authority Congress gave it to regulate communications." *Huawei Technologies USA, Inc. v. FCC*, 2 F.4th 421, 427(5th Cir. 2021).

[37] *See Supply Chain Order*, 34 FCC Rcd at 11438-48, paras. 43-63. In this order, the Commission noted that section 889(f)(3) of the 2019 NDAA had discussed in the context of that law that "covered telecommunications equipment" included equipment produced by Huawei, ZTE, Hytera, Hikvision, and Dahua. *Id.* at 11427, para. 13.

254 of the Communications Act of 1934, as amended,[38] the Commission noted that its actions were supported by the goals of section 889 of the 2019 NDAA (which, as noted above, prohibits executive agencies from, among other things, procuring or obtaining certain equipment or services identified as "covered telecommunications equipment or services" as defined in section 889).[39] The Commission also adopted a broad prohibition on the use of universal service funds (USF) to procure or otherwise support "any and all equipment and services produced or provided by" a covered company, stating that a blanket prohibition best promoted national security, provide regulatory certainty, and reduce regulatory burdens and administrative costs for both providers (that use USF support) and customers.[40] In addition, the Commission established a process to finalize these initial designations and to issue future designations of other companies posing such a risk.[41] Consistent with that process,[42] the Commission's Public Safety and Homeland Security Bureau (PSHSB) issued final designations of Huawei and ZTE as covered companies on June 30, 2020,[43] which immediately precluded use of USF support to purchase, maintain, improve, modify, operate, manage, or otherwise support any equipment or services produced or provided by Huawei or ZTE or their subsidiaries, parents, or affiliates.[44]

18. In July 2020, the Commission adopted its *Supply Chain Declaratory Ruling and Second Further Notice*, which found that the Commission's prohibition on the use of USF support to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services produced or provided by any company posing a national security threat to the integrity of communications networks or the communications supply chain, codified at 47 CFR § 54.9, "is consistent with and substantially implements subsection 3(a) of the Secure Networks Act, which prohibits the use of federal funds on certain communications equipment and services."[45] The Commission also sought comment on how other

[38] *See* 47 U.S.C. §§ 201(b), 254.

[39] *See Supply Chain Order*, 34 FCC Rcd at 11437-38, para. 38; *see also id.* at 11427, para. 13 (discussing section 889 of the 2019 NDAA). The Commission had sought comment on how to interpret section 889 of the 2019 NDAA in that proceeding. *Id.* at 11432, para. 25.

[40] *Supply Chain Order*, 34 FCC Rcd at 11449-50, paras. 67-69.

[41] *See id.*, 34 FCC Rcd at 11449, paras. 64-65.

[42] *See id.*, 34 FCC Rcd at 11438, para. 40; *id.* at 11449, para. 64; *id.* at 11486, para. 185 (directing the Public Safety and Homeland Security Bureau to determine whether to finalize the initial designations within 120 days of the Order's publication in the Federal Register, and holding that the Bureau may extend the 120-day deadline for good cause); *Public Safety and Homeland Security Bureau Extends Timeframe For Determining Whether to Finalize Designations of Huawei and ZTE Pursuant to 47 CFR § 54.9*, PS Docket Nos. 19-351 and 19-352, Public Notice, 35 FCC Rcd 4515 (PSHSB 2020) (finding good cause to extend the timeframe for determining whether to finalize the initial designations of Huawei and ZTE to June 30, 2020).

[43] *See generally Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation*, PS Docket No. 19-351, Order, 35 FCC Rcd 6604 (PSHSB 2020) (*Huawei Designation Order*); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – ZTE Designation*, PS Docket No. 19-352, Order, 35 FCC Rcd 6633 (PSHSB 2020) (*ZTE Designation Order*).

[44] *See generally Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation*, PS Docket No. 19-351, Order, 35 FCC Rcd 6604 (PSHSB 2020); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – ZTE Designation*, PS Docket No. 19-352, Order, 35 FCC Rcd 6633 (PSHSB 2020). Section 54.9(a) of the Commission's Rules states: "No universal service support may be used to purchase, obtain, maintain, improve, modify, or otherwise support any equipment or services produced or provided by any company posing a national security threat to the integrity of communications networks or the communications supply chain." 47 CFR § 54.9(a).

[45] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Declaratory Ruling and Second Further Notice of Proposed Rulemaking, 35 FCC Rcd 7821, 7826-27, para. 20 (2020) (*2020 Supply Chain Declaratory Ruling and Second Further Notice*).

sections of the Secure Networks Act interact with the Commission's ongoing efforts to secure the communications supply chain.[46]

19. In December 2020, the Commission adopted its *Supply Chain 2nd R&O*, in which it took further steps toward securing our communications networks and implementing provisions of the Secure Networks Act that apply to Commission action directed toward securing our nation's communications networks.[47] A core component of that decision involved creation and publication of the Covered List.[48] The Commission noted that under the statute it had no discretion to disregard determinations from any of the four enumerated sources identified in the Secure Networks Act, and that the Commission could accept determinations only from these four sources.[49] The Commission also noted that the "covered" equipment on the Covered List could identify specific pieces of equipment or include a class or category of equipment,[50] and that the Commission was not required to conduct a technical analysis of the equipment prior to including it on the Covered List.[51] In the *Supply Chain 2nd R&O*, the Commission adopted a new part 1 section in its rules, section 1.50000 *et seq*., to implement particular provisions in the Secure Networks Act. These include rules on listing "covered" equipment on the Covered List published by PSHSB and updating that list, establishing and implementing the Reimbursement Program to assist providers of advanced communications service with the costs of removing, replacing, and disposing of certain "covered" equipment and services, and the annual reporting requirement in which advanced communications service providers must report "covered" equipment or services.[52] Consistent with section 3 of the Secure Networks Act, the Commission also updated its rules (section 54.10) to prohibit use of Federal subsidies made available through a program administered by the Commission that provides funds to be used for the capital expenditures necessary for the provision of advanced communications service to purchase, rent, lease, otherwise obtain or maintain any "covered" communications equipment

[46] *See id.* at 7828-39, paras. 23-60.

[47] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Second Report and Order, 35 FCC Rcd 14284 (2020) (*Supply Chain 2nd R&O*).

[48] *Id.* at 14311-12, para. 58 (quoting the Secure Networks Act § 2(c)).

[49] *Id.* at 14312, para. 60 (citing the Secure Networks Act § 2(c) ("In taking action under subsection (b)(1), the Commission shall place on the list any communications equipment or service that poses an unacceptable risk to the national security of the United States or the security and safety of United States persons based solely on one or more of the following determinations . . . ."). *See also id.* at 14312-16, paras. 61-70.

[50] *Id.*at 14312, para. 59. The Commission noted that if interested parties seek to reverse or modify the scope of one of the determinations, the party should petition the source of the determination. *Id.*at 14324, para. 89. Meanwhile, with regard to *broader* determination, such as a class or category of communication equipment or service (e.g., "telecommunications equipment produced or provided by Huawei Technologies Company" or any subsidiary or affiliate), or telecommunications equipment that "is capable of (A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles, (B) causing the networks of a provider of advanced communications service to be disrupted remotely, or (C) otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons" – that broader category will be included on the Covered List. *Supply Chain 2nd R&O*, 35 FCC Rcd at 14321, paras. 82-83 (citing the Secure Networks Act §§ 2(b)(1); 2(b)(2)(A)-(C)). The Commission noted that, by adopting this approach and continuing to be deferential to the enumerated sources making the determination, the Commission will continue to work closely with Executive Branch entities with expertise and responsibilities concerning telecommunications security, including supply chain security. *Id.*at 14321, para. 83. The Commission disagreed with those that argued that broad or general categories of equipment should not be included on the Covered List and rejected the view that the specified agencies must identify particular pieces or categories of equipment that posed an unacceptable risk. *Id.*at 14322, para. 84.

[51] *Id.*at 14322, para. 85. The Commission also noted that the Covered List would be published without providing notice or opportunity to comment. *Id.* at 14317, para. 72.

[52] *See generally* 47 CFR §§ 1.50000 *et seq.*

or service on PSHSB's Covered List.[53] Pursuant to section 5 of the Secure Networks Act and section 1.50007 of the Commission's rules, all advanced communications service providers must submit the "Supply Chain Annual Report" requiring them to certify whether they had purchased, rented, leased or otherwise obtained "covered" equipment or services.[54]

20. In July 2021, the Commission adopted the *Supply Chain 3rd R&O*.[55] In this decision, the Commission provided additional guidance on, and directed changes to, the Commission's Reimbursement Program concerning certain "covered" communications equipment and services. The Commission found that the Consolidated Appropriations Act (CAA) of 2021, amended the Secure Networks Act, "to limit the acceptable use of Reimbursement Program funds to the removal, replacement, and disposal of eligible equipment and services that are both: (1) on the Covered List published pursuant to section 2(a) of the Secure Networks Act; and (2) as captured by the definition of equipment or services established in the *2019 Supply Chain Order*, or as determined by the process set forth in section 54.9 of the Commission's rules and in the *Designation Orders*."[56] Applying these factors, the Commission concluded that communications equipment and services produced or provided by Huawei or ZTE and obtained by eligible providers of advanced communications on or before June 30, 2020 would be eligible for support in the Reimbursement Program,[57] rather than all of the equipment and services on the initial Covered List published earlier that year, in March 2021, which had also included equipment and services produced or provided by the three other entities (Hytera, Hikvision, and Dahua).[58]

21. By May 5, 2022, advanced communications services providers were required to submit their first annual "Supply Chain Annual Report" on whether they had purchased, leased, rented, or otherwise obtained "covered" equipment on or after August 14, 2018.[59] In particular, all providers must answer whether they do or do not have "covered" equipment or services to report, and to certify that their

[53] *Supply Chain 2nd R&O*, 35 FCC Rcd at 14325-30, paras. 93-105; 47 CFR § 54.10.

[54] *Supply Chain 2nd R&O*, 35 FCC Rcd at 14369, para. 212; 47 CFR § 1.50007.

[55] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Third Report and Order, 36 FCC Rcd 11958 (2020) (*Supply Chain 3rd R&O*).

[56] *Id.*at 11965, 11969, paras. 19, 28.

[57] *Id.*at 11965, 11970-71, paras. 19, 30.

[58] *Id.*at 11971-72, paras. 31-32. Section 54.11 of the Commission's rules requires that eligible telecommunications carriers receiving universal service support certify that they do not use "covered communications equipment or services" prior to receiving a funding commitment or support. 47 CFR § 54.11(a). In the *Supply Chain 3rd R&O*, the Commission aligned the scope of "covered communications equipment or services" under this rule with the scope of "covered communications equipment or services" that must be removed or replaced by Reimbursement Program participants *Supply Chain 3rd R&O*, 36 FCC Rcd at 11965, 11974, paras. 19, 37. Accordingly, the certification requirement in section 54.11 of the Commission's rules applies to all communications equipment produced and provided by Huawei or ZTE, *Supply Chain 3rd R&O*, 36 FCC Rcd at 11965, 11974, paras. 19, 37, n.118.

[59] The Office of Economics and Analytics announced the first annual reporting requirement on February 4, 2022 and providers were required to submit the first certification by May 5, 2022. Specifically, in the annual reports all providers of advanced communications service were required to certify whether they had purchased, rented, leased or otherwise obtained covered equipment or services – in the case of equipment and services on the initial Covered List, or on or after 60 days after new "covered" equipment or services are added to the list. Providers that certify that they have obtained covered equipment or services are required to submit information on the location of the equipment or service; date the equipment or service was procured; removal or replacement plans for the equipment or service, including cost to replace; amount paid for the equipment or service; the supplier for the equipment or service; and a detailed justification for obtaining such covered equipment and service. *Office of Economics and Analytics and Wireline Competition Bureau Announce the Establishment of the Supply Chain Annual Reporting Portal*, Public Notice, DA 22-109, 2022 (OEA & WCB Feb. 4, 2022) (*Supply Chain Annual Report Public Notice*).

answer is truthful and accurate.[60] Several noted that they had purchased or otherwise obtained "covered" equipment, including telecommunications equipment (e.g., network equipment, including core, distribution, and access layers) and video surveillance equipment produced by entities identified on the current Covered List as producers of "covered" equipment.[61]

22. *The Covered List.* As noted above, pursuant to the Secure Networks Act and section 1.50002(a) of the Commission's rules, PSHSB is required to publish the "Covered List," which identifies "covered communications equipment or service" that has been determined, by one or more of four enumerated sources outside of the Commission, as posing an unacceptable risk to the national security of the United States or the security and safety of United States persons.[62] The Commission tasked PSHSB with ongoing responsibilities for monitoring the status of the determinations and periodically updating the Covered List to address changes as appropriate.[63]

23. On March 12, 2021, PSHSB published its first Public Notice on the Covered List.[64] That list specifically identified equipment and services that, pursuant to the Secure Networks Act, had been determined by Congress in section 889(f)(3) of the 2019 NDAA – one of the four enumerated sources identified under the Secure Networks Act[65] – as posing an unacceptable risk to national security.[66] Among others things, that Covered List listed as "covered" equipment certain equipment produced by five different entities: Huawei, ZTE, Hytera, Hikvision, and Dahua (and their respective subsidiaries and affiliates). On March 25, 2022, PSHSB published a Public Notice updating the Covered List; this list retained the earlier identified "covered" equipment (equipment produced by Huawei, ZTE, Hytera, Hikvision, and Dahua) while announcing additions to the Covered List based on new determinations by two of the other enumerated sources,[67] DHS and an executive branch interagency body (Team Telecom) with appropriate expertise.[68] Most recently, on September 20, 2022, PSHSB published another Public Notice updating the Covered List; this list also retained the earlier identified "covered" equipment (equipment produced by Huawei, ZTE, Hytera, Hikvision, and Dahua) while announcing certain additions to the Covered List based on new determinations by the Department of Justice, in coordination and concurrence with the Department of Defense.[69]

---

[60] 47 CFR § 1.50007(a)(6).

[61] This information is based on Commission staff review.

[62] Secure Networks Act § 2(d).

[63] *See Supply Chain 2nd R&O*, 35 FCC Rcd 14284 (the Commission created and interpreted the Secure Networks Act's Covered List requirement, promulgating 47 CFR § 1.50002).

[64] *Public Safety and Homeland Security Bureau Announces Publication of the List of Equipment and Services Covered by Section 2 of the Secure Networks Act*, WC Docket 18-89, Public Notice, 36 FCC Rcd 5534 (PSHSB 2021) (*2021 Covered List Public Notice*).

[65] Secure Networks Act § 2(c)(3).

[66] *2021 Covered List Public Notice*, 36 FCC Rcd at 5535-36.

[67] Secure Networks Act § 2(c)(1) and (4).

[68] *Public Safety and Homeland Security Bureau Announces Additions to the List of Equipment and Services Covered by Section 2 of the Secure Networks Act*, WC Docket No. 18-89, Public Notice (PSHSB Mar. 21, 2022) (*March 2022 Covered List Public Notice*) at 1-2 & Appendix. PSHSB maintains the Covered List at https://www.fcc.gov/supplychain/coveredlist.

[69] *Public Safety and Homeland Security Bureau Announces Additions to the List of Equipment and Services Covered by Section 2 of the Secure Networks Act*, WC Docket No. 18-89, Public Notice (PSHSB Sept. 20, 2022) (*September 2022 Covered List Public Notice*) at 1-2 & Appendix. PSHSB maintains the Covered List at https://www.fcc.gov/supplychain/coveredlist.

B. The *NPRM* and *NOI*

24. The Commission adopted an *NPRM* and an *NOI* on June 17, 2021. This initiated two separate dockets, with one docket concerning revisions to the Commission's equipment authorization program and the other concerning the Commission's competitive bidding program. In the *NOI*, the Commission sought broad comment on possible additional steps that it could take to leverage the equipment authorization program to promote cybersecurity.

25. *NPRM concerning the Equipment Authorization Program (ET Docket No. 21-232).* The Commission's equipment authorization rules play a critical role in enabling the Commission to carry out its responsibilities under the Communications Act. The Commission's equipment authorization program, codified in part 2 of its rules, promotes efficient use of the radio spectrum and addresses various responsibilities associated with certain treaties and international regulations,[70] while ensuring that RF devices in the United States comply with the Commission's technical requirements before they can be marketed in or imported to the United States.[71] As a general matter, for an RF device to be marketed or operated in the United States, it must have been authorized for use by the Commission,[72] although a limited number of categories of RF equipment are exempt from this requirement.[73]

26. In the *NPRM*, the Commission proposed to revise its equipment authorization program under its part 2 rules to prohibit authorization of "covered" equipment on the Commission's Covered List, i.e., equipment that had been determined to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons.[74] To achieve this goal, the Commission proposed to revise the rules and procedures for its two pathways for equipment authorization – certification and the Supplier's Declaration of Conformity (SDoC).[75] Recognizing that "covered" equipment might also include some equipment that is currently exempted from authorization requirements, the Commission sought comment on whether such exemptions should continue.[76] The Commission also sought comment on whether any existing equipment authorization of "covered" equipment should be revoked, and if so, under what procedures.[77] The Commission noted that adopting rules that take security into consideration in the equipment authorization process would serve the public interest by addressing significant national security risks that had been identified, and would be consistent with the Commission's statutory "purpose of regulating interstate and foreign commerce in communications by wire and radio ... for the purpose of the national defense [and] for the purpose of

---

[70] 47 CFR § 2.901.

[71] *See* 47 CFR part 2 subpart I, §§ 2.801 *et seq*. (Marketing of Radio Frequency Devices); part 2 subpart J, §§ 2.901 *et seq*. (Equipment Authorization Procedures); part 2 subpart K, §§ 2.1201 *et seq*. (Importation of Devices Capable of Causing Harmful Interference). The Office of Engineering and Technology (OET) administers day-to-day operation of the equipment authorization program. *See* 47 CFR § 0.241(b). OET's Laboratory Division maintains a webpage devoted to the equipment authorization program. See the FCC's, Equipment Authorization Approval Guide, https://www.fcc.gov/engineering-technology/laboratory-division/general/equipment-authorization.

[72] 47 CFR §§ 2.803(b) and 2.805(a).

[73] *See, e.g.*, 47 CFR § 15.103. For background on exempt equipment, see the *NPRM*, 36 FCC Rcd at 10593-94, para. 31.

[74] *NPRM*, 36 FCC Rcd at 10596, para. 40.

[75] *Id.* at 10598-10606, paras. 44-64. More specifically, these two approval processes are: (1) Certification by an FCC-recognized Telecommunication Certification Body (TCB) for RF devices with the greatest potential to cause harm to consumers or other radio operations; and (2) a Supplier's Declaration of Conformity (SDoC), a self-certification whereby the responsible party determines that the equipment has been shown to comply with the applicable technical standards. For background on the Certification of Equipment process, see *NPRM* 36 FCC Rcd at 10592-93, paras, 28-29. For background on the SDoC process, see *NPRM*, 36 FCC Rcd at 10593, para. 30.

[76] *NPRM*, 36 FCC Rcd at 10608-10, paras. 73-79.

[77] *Id.* at 10611-15, paras. 80-97.

promoting safety of life and property."[78] It tentatively concluded that the Commission has the authority to prohibit authorization of equipment on the Covered List, pointing to section 302 of the Communications Act of 1934, sections 303(e), and other bases, including the Communications Assistance for Law Enforcement Act (CALEA), as well as ancillary authority under section 4(i) of the Act.[79]

27. Several commenters generally support the Commission's overall goal and proposed approach with regard to prohibiting authorization of "covered" equipment,[80] while others disagree with the Commission's proposal and challenge its legal authority to proceed.[81] Many express concern that any action that the Commission takes should be designed so as not to cause disruption or delay in the authorization of equipment that does not raise national security concerns.[82] Many commenters also oppose action by the Commission to revoke existing authorizations of "covered" equipment, expressing various concerns such as the potential for adverse impact to consumers and the supply chain.[83]

28. *NPRM on Competitive Bidding Program (EA Docket No. 21-233).* The Commission uses competitive bidding (i.e., auctions) to determine which among multiple applicants with mutually exclusive applications for a license may file a full application for the license.[84] Pursuant to this authority, the Commission has required each applicant that participates in competitive bidding to make various certifications.[85] These required certifications address a range of public interest concerns related to the conduct of competitive bidding and the national security interest in precluding some parties from

[78] *Id.*at 10611, para. 65.

[79] *Id.*at 10606-08, paras. 65-69.

[80] *See, e.g.*, China Tech Threat and Blue Path Labs (China Tech Threat) Comments at 45-46; NCTA Comments at 4-5; TIA Comments at 10; Coalition for a Prosperous America Comments at 1-2; IPVM Reply Comments at 5; JVCKenwood Comments at 2; Jordan Brunner Comments at 23..

[81] *See, e.g.*, Dahua Technology USA (Dahua USA) Comments at 4 (no provision of the Communications Act gives the Commission authority to prohibit authorization of equipment based solely on the identity of the manufacturer); Hikvision USA Comments at 2 (the Commission lacks authority to adopt its proposed rule); Huawei Comments at 18 (the Commission cannot identify any explicit source of authority to implement categorical ban under the established equipment authorization procedures); CTA Comments at 37 (the silence of the Secure Networks Act calls into question the FCC's ability to act as proposed); NTCA Reply Comments at 2 (even those who asserted that the Commission should adopt the proposed rules failed to provide any existing legal basis for such action).

[82] *See*, *e.g.*, CTA Comments at 12 (the proposal could burden "good actor" companies with no guarantee of a national security benefit.); CTIA Comments at 9 (the *NPRM* proposes to add additional requirements that reach beyond identified national security threat actors; the Commission should ensure that any new rules are narrowly tailored to known threats and are still able to promote the equipment authorization regime's longstanding goals); NCTA at 5 (the proposal significantly expands the number and types of equipment subject to the Commission's equipment authorization process; the time needed for manufacturers to make the required certification for all of their communications equipment and for the Commission to process the additional certifications will almost certainly result in a delay prior to such equipment being commercially available).

[83] *See*, *e.g.*, 5G Americas Comments at 2 (does not support retroactive rescission); Consumer Technology Association (CTA) Comments at 14 (could be disastrous for consumers); CTIA Comments at 9-12 (could present serious challenges potentially harming American consumers, and could weaken supply chains); ITI Council Comments at 5-8 (revocation of "covered" equipment would unmoor the revocation process, present a myriad of practical challenges as well as industry and consumer confusion); NCTA – the Internet & Television Association (NCTA) Comments at 9-10 (would create an unfunded "rip" and "replace" mandate); NTCA Comments at 7 (would be highly detrimental to providers that relied on the Commission's rules); Telecommunications Industry Association (TIA) Comments at 12 (only proceed if a mechanism exists to reimburse those affected).

[84] *See* 47 U.S.C. § 309(j).

[85] 47 CFR § 1.2105(a)(2)(iv)-(xiii).

obtaining licenses through competitive bidding.[86] Parties unable to make the required certifications have their applications to participate dismissed.[87]

29. In the *NPRM*, the Commission sought comment on requiring any entity participating in the Commission's competitive bidding processes to certify that its bid does not and will not rely on financial support from any entity that the Commission has designated, under section 54.9 of its rules, as a national security threat to the integrity of communications networks or the communications supply chain. Under those existing rules, Huawei and ZTE and their parents, affiliates, and subsidiaries have been so designated.[88] Without fully supporting or opposing the certification discussed in the *NPRM*, four parties filed comments offering varying suggestions for how the Commission might proceed with such a certification.[89]

30. *NOI on Equipment Authorization Program (ET Docket No. 21-232).* In the *NOI*, the Commission sought broad comment on other possible actions the Commission could take to create incentives in equipment authorization processes for improved trust through the adoption of cybersecurity best practices in consumer devices. Although a few commenters support certain Commission actions to leverage its equipment authorization program to further promote improved cybersecurity practices,[90] most commenters oppose Commission action on its own and instead support a broader, "whole of government" approach in which the Commission could contribute.[91]

C. The Secure Equipment Act of 2021

31. On November 11, 2021, subsequent to the Commission's adoption of the *NPRM and NOI*, the President signed and enacted into law the Secure Equipment Act of 2021 (Secure Equipment Act). This Act specifically concerns the Commission's equipment authorization program in the instant proceeding (ET Docket No. 21-232),[92] in which the Commission has proposed prohibiting future authorizations of equipment on the Commission's Covered List published under section 2(a) of the Secure Networks Act. In section 2(a)(1), the Secure Equipment Act provides that, not later than one year

[86] *See* 47 CFR § 1.2105(a)(2)(ix) (regarding joint bidding arrangements) and (xiii) (regarding bars against participation in certain auctions based on national security).

[87] *Id.* § 1.2105(b)(1).

[88] *See Public Safety and Homeland Security Bureau Issues Final Designations of Huawei Technologies Company and ZTE Corporation as Companies Posing a National Security Threat to the Integrity of Communications Networks and the Communications Supply Chain Pursuant to 47 CFR § 54.9*, PS Docket Nos. 19-351, 19-352, Public Notice, 35 FCC Rcd 6602 (PSHSB 2020). *In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – ZTE Designation,* PS Docket Nos. 19-352, Memorandum Opinion and Order, 35 FCC 131416 (PSHSB 2020)(denying Petition for Reconsideration), *In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation,* PS Docket Nos. 19-351, Memorandum Opinion and Order, FCC 20-179, 2020 WL 7351129 (2020)(denying Application for Review).

[89] *See*, *e.g.*, CTIA comments at 2; US Telecom Comments at 6; Jordan Brunner Comments at 28; JVCKenwood Comments at 11.

[90] *See*, *e.g.*, David Simpson Comments at 2 (Commission engagement will provide a positive stimulus and focal point for the identification and incorporation of device level cybersecurity best practices); Charter Reply Comments at 5 (Commission should leverage its equipment authorization program by requiring device manufacturers to include safeguards against major cybersecurity vulnerabilities).

[91] *See*, *e.g.*, CTIA Comments at 3; ACT – The App Association, CTA, Council to Secure the Digital Economy, CTIA, ITA, TIA, and US Telecom Comments at 3; ITI Comments at 16; NTCA Comments at 3.

[92] Secure Equipment Act § 2(a)(1).

after the date of its enactment, the Commission "shall adopt rules" in the [instant] proceeding."[93] In section 2(a)(2), the Act provides:

> [T]he Commission shall clarify that [it] will no longer review or approve any application for equipment authorization for equipment that is on the list of covered communications equipment or services published by the Commission under section 2(a) of the [Secure Networks Act].[94]

In section 2(a)(3)(A), the Act further provides that:

> In the rules adopted … the Commission may not provide for review or revocation of any equipment granted before the date on which such rules are adopted on the basis of the equipment being on the list described [above].[95]

Finally, in section 2(a)(3)(B), the Act states:

> Nothing in [the Secure Equipment Act] may be construed to prohibit the Commission, other than the rules adopted under [section 2(a)(1)], from –
> (i) examining the necessity of review or revocation of any equipment authorization on the basis of the equipment being on the list described [above]; or
> (ii) adopting rules providing for any such review or revocation.[96]

III. REPORT AND ORDER

32. In this Report and Order, we build upon ongoing efforts by Congress, the Executive Branch, and the Commission to protect our nation's networks and supply chains from equipment and services that pose an unacceptable risk to national security or the safety of U.S. persons. Consistent with our proposals in the *NPRM* (ET Docket No. 21-232), we adopt several revisions to the Commission's equipment authorization program to prohibit authorization of "covered" equipment identified on the Commission's Covered List in order to protect our nation's communications systems from equipment that has been determined to pose an unacceptable risk. Our actions today fulfill Congress's mandate that the Commission adopt such rules within one year of enactment of the Secure Equipment Act of 2021. They also lay the foundation for future actions by the Commission to implement prohibitions in our equipment authorization program that will serve to protect the American people.

33. We first find that the Commission has clear legal authority, as underscored by the Secure Equipment Act, for modifying the Commission's equipment authorization program to prohibit authorization of "covered" equipment identified on the Commission's Covered List. We then discuss several rule revisions that we are adopting in our equipment authorization program (administered under part 2 of the Commission's rules) that will serve to prohibit the authorization of "covered" equipment, whether that equipment is listed on the current Covered List or is listed subsequently on an updated Covered List based on any future determinations made by our nation's national security agencies. We also discuss the Covered List, including the statutory framework associated with the list, the "covered" equipment on the current Covered List that we are prohibiting from authorization, and how additional "covered" equipment identified in future updates to the Covered List will be prohibited from authorization under our equipment authorization program. Finally, we address other issues raised by commenters (e.g., cost-effectiveness and constitutional claims), as well as provide an overview of the Commission's anticipated outreach efforts to inform manufacturers, industry, other interested parties, and the public that will be affected by the actions to protect the American public through elimination from the United States' equipment supply chain of equipment that poses an unacceptable risk to national security.

---

[93] *Id.* § 2(a)(1).

[94] *Id.* § 2(a)(2).

[95] *Id.* § 2(a)(3)(A).

[96] *Id.* § 2(a)(3)(B).

A. Legal Authority to Address Security Concerns through the Equipment Authorization Program

34. In the *NPRM*, the Commission stated that adopting rules that take security into consideration in the equipment authorization process would serve the public interest by addressing significant national security risks that have been identified by the Commission in other proceedings, and by Congress and other federal agencies, and would be consistent with the Commission's broad statutory authority.[97] The Commission sought comment on its tentative conclusion that, although not specifically authorized by the Secure Networks Act, the Commission has sufficient broad authority to adopt its proposals in the *NPRM*.[98]

35. The Commission received a range of comments and reply comments on its legal authority during the comment period in this proceeding.[99] Some commenters argue that the Secure Networks Act provides the Commission clear authority to adopt its proposals.[100] Other commenters, including representatives of some of the companies named on the then-current Covered List (Huawei, Hikvision, and Dahua), argue that there is no legal basis in the Secure Networks Act for the Commission to take the proposed actions.[101] Additionally, a few commenters argue the Secure Networks Act provides the Commission very limited authority to amend the part 2 rules.[102]

36. On November 11, 2021, President Biden signed into law the Secure Equipment Act.[103] The Secure Equipment Act requires that, by November 11, 2022, the Commission adopt rules in the instant proceeding (ET Docket 21-232) to update "the equipment authorization procedures of the Commission" to "clarify that the Commission will no longer review or approve any application for

---

[97] *NPRM*, 36 FCC Rcd at 10606, para. 65; *see id.* at 10607-08, paras. 66-69.

[98] *See generally id.* at 10606-08, paras. 65-69.

[99] Comments were due on September 20, 2021, and reply comments were due on October 18, 2021.

[100] *See, e.g.*, Telecommunications Industry Association (TIA) Comments at 5; TIA Reply Comments at 6-7; China Tech Threat and Blue Path Labs (China Tech Threat) Comments at 44-45; Motorola Solutions, Inc. (Motorola) Reply Comments at 4 (the Secure Networks Act provides the Commission with the authority to prohibit the authorization of equipment on the Covered List in order to ensure the equipment at issue is not utilized in the networks of entities receiving Universal Service Fund support); JVCKenwood USA Corporation (JVCKenwood) Comments at 5-6 (the Secure Networks Act, along with other legislation, executive orders, and Commission precedent, provide the authority to adopt the proposals, and the ability to deploy Covered List equipment is contrary to established federal policy and national security interests); Shane Tews Reply Comments at 1-3 (Secure Networks Act, along with the Communication Act and the Commission's rules, provide the authority to adopt the proposals).

[101] *See*, *e.g.*, Huawei Technologies Co. Ltd. and Huawei Technologies USA (Huawei Cos.) Comments at 18-34; Hikvision USA Comments at 4-7, 27-32; Dahua USA Comments at 5-14 (no statute explicitly gives the Commission any authority, responsibility, or direction to withhold or revoke equipment authorizations based on national security considerations).

[102] *See*, *e.g.*, NCTA Comments at 3-4 (the Commission's limited authority to act under the Secure Network Act does not support its taking more granular and intrusive action than is warranted by the statute, such as applying the prohibition proposed in the *NPRM* to any individual components or software elements; NCTA suggests that a risk management approach, such as that employed by the national security agencies in addressing supply chain risks, would be a more prudent way to tackle a prohibition on authorization of Covered List equipment); Hytera US Comments at 17 (Commission may not exceed authority granted by Congress); NTCA Comments at 1-4 (Commission's proposed action exceeds the scope of the Commission's authority under section 302 of the Communications Act, which limits the Commission's authority to adopt regulations on equipment authorization to address RF and interference-related issues; NTCA acknowledged, however, that Congress could amend the Secure and Trusted Communications Networks Act to require manufacturers to certify that their equipment is not "covered"); Hikvision USA Comments at 27-50 and Dahua USA Comments at 5-14 (Commission lacks express or ancillary authority to adopt proposals in *NPRM*).

[103] *See* Section II.C (discussing the Secure Equipment Act).

authorization of equipment that is on the list of covered communications equipment or services" (*i.e.*, the Covered List), and "to update the equipment authorization procedures of the Commission" accordingly.[104]

37. Some commenters subsequently filed *ex parte* letters specifically discussing the Secure Equipment Act. CTA contends that the Secure Equipment Act unequivocally resolves that we have authority to act on our proposals to block future applications for authorization of "covered" equipment on the Covered List, and confirms that the Commission should move forward expeditiously with its proposal.[105] While Hytera Ltd. and Hytera US, Hikvision USA, and Dahua USA do not dispute the Commission's legal authority to prohibit authorization of "covered" equipment appropriately placed on the Covered List, they each maintain that the Commission's authority under the Secure Networks Act and the Secure Equipment Act precludes the Commission from adopting equipment authorization prohibitions on the equipment that they produce.[106]

38. We find that we have authority to adopt the proposals in the *NPRM* with regard to prohibiting authorization of "covered" equipment on the Covered List. We reach this determination based on two grounds.

39. First, we find that the Secure Equipment Act provides the Commission with express authority to adopt rules that prohibit the review or approval of any application for equipment authorization for equipment that is listed on the Commission's Covered List and requires the Commission to act. Section 2(a)(1) of the Secure Equipment Act expressly states that, no later than one year after its enactment, the Commission shall adopt rules in the instant proceeding to do so. By determining here – as specified in more detail below – that the agency will no longer review or approve any equipment authorization for equipment that is on the Commission's Covered List, the Commission is acting based on the clear and express statutory language contained in section 2(a)(1) of the Secure Equipment Act. Thus, the Commission has legal authority to adopt those rules.

40. Second, the Commission has legal authority to take the relevant equipment authorization actions to prohibit authorization of "covered" equipment specified in this Report and Order (as well as with regard to revocation of authorizations discussed below[107]) based on the agency's statutory authority that predates Congress's 2021 enactment of the Secure Equipment Act. Before that enactment, the Commission's *NPRM* in this proceeding relied on a number of preexisting statutory provisions to support this view. We continue to believe, as noted in the *NPRM,* that section 302 of the Communications Act provides additional authority to adopt the rule and procedure changes proposed in the *NPRM*. The directive in section 302 to, "consistent with the public interest, convenience, and necessity, make reasonable regulations … governing the interference potential of devices which in their operation are capable of emitting radio frequency energy by radiation, conduction, or other means in sufficient degree to cause harmful interference to radio communications," gives us authority to implement other statutory responsibilities.[108] And the inclusion of the phrase "public interest" in section 302(a) provides independent authority to take into account, in our consideration of the public interest, the national defense, and the promotion of safety of life and property, goals which must inform the Commission's

[104] Secure Equipment Act §§ 2(a)(1)-(2).

[105] CTA December 16, 2021 *Ex Parte* at 3. We also note that two commenters stated in their comments filed in September 2021 that, were the then-pending Secure Equipment Act ultimately enacted into law, that Act would bolster the Commission's assertion in the *NPRM* of its legal authority in this proceeding. Johnson/Tatel Comments at 2-4.

[106] *See*, *e.g.*, Hytera Ltd. May 13, 2022 *Ex Parte* at 2; Hikvision USA Feb. 23, 2022 *Ex Parte* at 5; Dahua USA Jan. 4, 2022 *Ex Parte* at 1-4.

[107] *See* Section III.B.6, below.

[108] *NPRM,* 36 FCC Rcd at 10607, para. 66.

exercise of its statutory responsibilities.[109] As explained extensively in this Report and Order, prohibiting authorization of equipment that has been placed on the Covered List is essential to the national defense and to the promotion of public safety. It is well-established that the promotion of national security is consistent with the public interest and part of the purpose for which the Commission was created. As section 1 of the Act states, the Commission was created "for the purpose of the national defense [and] for the purpose of promoting safety of life and property through the use of wire and radio communication …."[110] And as the Supreme Court has instructed, we do not read any "particular statutory provision in isolation," but rather "in [its] context and with a view to [its] place in the overall statutory scheme."[111]

41. In this regard, as further noted in the *NPRM* issued prior to the Secure Equipment Act, the Commission's statutory authority also included the authority under section 303(e) of the Communications Act to "[r]egulate the kind of apparatus to be used with respect to "its external effects" (among other things).[112] Further, as suggested in the *NPRM,* section 105 of the Communications Assistance for Law Enforcement Act (CALEA) supports the Commission's authority to prescribe the rules that we adopt in this Report and Order. That section requires telecommunications carriers to ensure that the surveillance capabilities built into their networks "can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission,"[113] and the Commission has concluded that its rule prohibiting the authorization of equipment on the Covered List that poses a national security threat implements that provision.[114] The Commission is required to prescribe rules necessary to implement CALEA's requirements, and we conclude that the rules we adopt here will help ensure that equipment that carriers include in their networks will not include such unlawful interception capabilities because use of equipment from companies that are identified by Congress and national security agencies to pose a national security threat is far more likely to be subject to unauthorized access. Finally, as noted in the *NPRM,* the Commission has ancillary authority to implement these statutory provisions by adopting such rules "as may be necessary in the execution of [these foregoing Commission] functions."[115]

42. Our reading of the Commission's pre-existing authority is confirmed by Congress's enactment of the Secure Equipment Act. By specifying both this proceeding, by its docket number, in referring expressly to "the Notice of Proposed Rulemaking" pending before the Commission, and by directing the Commission to "clarify" that it would no longer review or approve any application for equipment that is on the Covered List, Congress clearly intended to ratify the Commission's tentative conclusions in the *NPRM* that it had authority as discussed therein.

43. For all these reasons, we now determine that the Commission has the requisite legal authority to take these actions. Indeed, the argument to the contrary can be summarized as follows: even though the Commission has authority to approve equipment for use in the United States, the Commission has no statutory discretion to determine not to authorize that equipment in the event that a national security agency determines that the equipment poses an unacceptable risk to our national security. We

---

[109] *See* 47 U.S.C. §§ 151, 302a(a); *NPRM*, 36 FCC Rcd at 10606, para. 65 & n.189. 47 U.S.C. § 303(e); *see NPRM*, 36 FCC Rcd at 10607, para. 66.

[110] 47 U.S.C § 151.

[111] *FDA v. Brown & Williamson Tobacco, Corp.,* 529 U.S. 120, 132-33 (2000).

[112] 47 U.S.C. § § 303(e); *NPRM,* 36 FCC Rcd at 10607, para. 66 & n.199. *See also* 47 U.S.C. § 303(g) (authority to "generally encourage the larger and more effective use of radio in the public interest"), *NPRM,* 36 FCC Rcd at 10606, para. 65 & n.192; 47 U.S.C. § 303(r) (authority to adopt rules "as may be necessary to carry out the provisions of [the Communications] Act").

[113] 47 U.S.C. § 1004; *NPRM,* 36 FCC Rcd at 10607-08, para. 68.

[114] *Cf. Supply Chain First Report and Order*, 34 FCC Rcd at 11436-37, paras. 35-36.

[115] 47 U.S.C. § 154(i); *NPRM,* 36 FCC Rcd at 10606, 10608, paras 65, 69 & n.190.

reject the argument that the foregoing collective sources of statutory authority – in the absence of the Secure Equipment Act – would have deprived the Commission of such discretion. And Congress expressly endorsed this view in the Secure Networks Act.

B. Revisions to the Equipment Authorization Program

44. In the *NPRM*, the Commission proposed to adopt revisions to its equipment authorization rules and processes to prohibit authorization of "covered" equipment on the Covered List.[116] The Commission proposed or sought comment on several potential revisions to various rule provisions related to the Commission's equipment authorization processes that would implement the proposed prohibition on authorization of equipment on the Covered List.[117] In particular, the Commission proposed or sought comment on revisions to the Commission's general part 2 rules and to specific provisions relating to authorization of equipment processed through the Commission's equipment certification and SDoC processes. We note at the outset that the Commission received numerous comments in support of its general objectives in proposing rules prohibiting authorization of equipment on the Covered List.[118] Several of these and other commenters also offer particular views on how the Commission should implement the prohibition, and some oppose significant elements of the proposal. We address the particular issues raised by commenters, below.

1. General provisions

45. In the *NPRM*, the Commission proposed to adopt, in the "General Provisions" section of its part 2, subpart J rules, a general prohibition of authorization of "covered" equipment identified on the Covered List. In particular, the Commission proposed to add new section 2.903 to clearly establish that the equipment on the Covered List – whether subject to the certification process or the SDoC process – would be prohibited from obtaining a Commission equipment authorization.[119] The Commission sought comment on the proposal and whether modifications or clarifications of the proposed new rule were needed.[120] In response, we received one comment expressing general support[121] and one of general opposition, largely arguing that the Commission lacks the authority to enact such a prohibition.[122] As discussed earlier in this item, Congress, through the Secure Equipment Act, directed the Commission to adopt rules, no later than November 11, 2022, to clarify that it would no longer review[123] or approve any

[116] *NPRM*, 36 FCC Rcd at 10596, para. 40.

[117] *Id.*at 10596-606, 10608-613, paras. 40-64, 73-89.

[118] *See, e.g.*, CTIA Comments at 1-3 (supports the Commission's important objectives); China Tech Threat Comments 3-4, 45-46 (supports Commission proposal to prohibit authorization of equipment on the Covered List); Jack Corrigan Comments & attached report by the Center for Security and Emerging Technology, "Banned in D.C.[:] Examining Government Approaches to Foreign Technology Threats" at 37 (federal policymakers must lead the effort to build a unified defense against foreign technology threats; the Commission's proposal to block authorization of equipment the Covered List is an important part of this effort); NCTA Comments at 2 (supports objectives underlying the *NPRM* proposals); TIA Comments at 2, 5 (supports banning authorization of equipment on the Covered List).

[119] *NPRM*, 36 FCC Rcd at 10597, para. 40.

[120] *Id.* at 10597-98, paras. 41-42.

[121] *See* Brunner Comments at 2.

[122] PR China Comments at 1 (the prohibition would violate the World Trade Organization Technical Barriers to Trade Agreement).

[123] The Commission interprets "review" in this context as relating only to the review of applications for the express purpose of obtaining equipment authorization. We do not interpret it to apply to such issues as responding to inquiries related to the equipment or requests for declaratory rulings.

application for authorization of equipment on the Covered List.[124] The Commission thus has an explicit statutory mandate to adopt such rules.

46. In accordance with the direction provided by the Secure Equipment Act, we adopt new rule 2.903 in subpart J of the Commission's part 2 equipment authorization rules.[125] This general prohibition makes clear that "covered" equipment identified on the Covered List will no longer be eligible for either of the two Commission equipment authorization procedures, certification or SDoC. In accordance with section 2(d) of the Secure Networks Act, the prohibition will extend to any communications equipment that is included in an updated Covered List in the future , and will no longer extend to any communications equipment that is removed from the Covered List. As discussed further in this item, this new provision also serves to prohibit marketing such equipment under subpart I of our rules and importation of such equipment under subpart K.

47. We also include within this new rule part additional general provisions associated with implementation of this prohibition in the Commission's equipment authorization program under part 2. These provisions include definitions to be used in connection with the Covered List (e.g., "subsidiary" and "affiliate"), as well the requirement that OET and PSHSB publish and maintain on the Commission's website information concerning on what constitutes "covered" equipment for purposes of implementing the prohibition on authorization of "covered" equipment.

2. Certification rules and procedures

48. In the *NPRM*, the Commission proposed several revisions to various rules and procedures concerning the certification of equipment, and sought comment on other potential revisions, in order to ensure that equipment on the Covered List would no longer receive equipment authorization.[126] The Commission noted that its intent is to revise the equipment authorization process in a way that efficiently and effectively prohibits authorization of "covered" equipment without delaying the authorization of innovative new equipment that benefits Americans' lives.[127] Thus, the Commission sought comment on "[w]hat information may be pertinent to assist the TCBs and the Commission in ensuring" against equipment authorization for such "covered" equipment, and on revisions to its rules that could better ensure compliance with those new requirements.[128]

49. As explained in the *NPRM*, the equipment certification procedures apply to certain radiofrequency devices that have the greatest potential to cause harmful interference to radio services.[129] Certification generally is required for equipment that consists of radio transmitters[130] as well as some unintentional radiators.[131] Examples of equipment that requires certification include wireless provider base stations, mobile phones, point-to-point and point-to-multipoint microwave stations, land mobile, maritime and aviation radios, wireless medical telemetry transmitters, Wi-Fi[132] access points and routers,

[124] *See* Secure Equipment Act.

[125] Appendix A, § 2.903.

[126] *See NPRM*, 36 FCC Rcd at 10598-603, paras. 44-56.

[127] *Id.*at 10600, para. 46.

[128] *Id.*at 10600, 1602-03, paras. 48, 54.

[129] *Id.*at 10598, para. 44.

[130] *See, e.g.*, 47 CFR §§ 25.129, 27.51, 95.361.

[131] 47 CFR § 15.101.

[132] Wi-Fi s a family of wireless network protocols, based on the IEEE 802.11 family of standards, which are commonly used for local area networking of devices and Internet access, allowing nearby digital devices to exchange data by radio waves.

home cable set-top boxes with Wi-Fi, and most wireless consumer equipment (e.g., tablets, smartwatches, and smart home automation devices).

50. Applicants for equipment certification are required to file their applications, which must include certain specified information,[133] with an FCC-recognized Telecommunications Certification Body (TCB).[134] The Commission, through its Office of Engineering and Technology (OET), oversees the certification process, and provides guidance to applicants, TCBs, and test labs with regard to required testing and other information associated with certification procedures and processes, including correspondence and pre-approval guidance provided via OET's knowledge database system (KDB).[135] Each applicant must provide the TCB with all pertinent information as required by the Commission's rules, including documentation that addresses compliance with the testing requirements that broadly apply to RF devices, specific technical requirements in particular service rules, and other applicable policy-related Commission requirements.[136] The TCB then evaluates the submitted documentation and test data to determine whether the device complies with the relevant Commission rules. Once a TCB grants an application, information about that authorization is publicly announced "in a timely manner" through posting on the Commission-maintained equipment authorization system (EAS) database, and referenced via unique FCC identifier (FCC ID). Certified equipment also is subject to various other requirements, including rules for modifying the equipment,[137] marketing the equipment,[138] and changing[139] or transferring ownership[140] of the associated FCC ID.

51. The Commission's goal is to revise the equipment authorization process in a way that efficiently and effectively prohibits authorization of covered equipment without delaying the authorization of innovative new equipment that benefits Americans' lives.[141] In the *NPRM*, the Commission proposed and sought comment on a requirement for each applicant for certification to make an attestation that the equipment is not "covered" equipment on the Covered List.[142] It also asked whether the applicant should be required to provide specific additional information that would help establish that the equipment is not "covered."[143] In addition, the Commission proposed that the party responsible for ensuring that equipment complies with applicable requirements be located within the United States and that the application for certification include relevant contact and address information.[144]

---

[133] *See* 47 CFR § 2.1033.

[134] 47 CFR §§ 2.907, 2.911; *see NPRM*, 36 FCC Rcd at 10598-99, para. 44. *See also* 47 CFR § 2.960.

[135] *See*, *e.g.*, 47 CFR §§ 2.947(a)(3), 2.1093(d)(2) which state that advisory information regarding measurement procedures can be found in the KDB, which is available at https://apps.fcc.gov/oetcf/kdb. Applications that involve new technology or for which there are no FCC-recognized test procedures require a TCB to obtain pre-approval guidance from the Commission before the application may be approved. *Id.*§ 2.964.

[136] *Id.*§§ 2.911, 2.1033.

[137] *Id.* §§ 2.932, 2.1043.

[138] *Id.* §§ 2.924, 2.1033(c)(20).

[139] *Id.* §§ 2.924, 2.933.

[140] *Id.* § 2.929.

[141] *NPRM*, 36 FCC Rcd at 10600, para. 46.

[142] *Id.* at 10600, para. 47.

[143] *Id.* at 10600, paras. 47-48.

[144] *Id.* at 10602-03, para. 54.

a. Attestation requirement

52. In the *NPRM*, the Commission specifically proposed to add a new provision to section 2.911 that would require applicants for certification to provide a written and signed attestation[145] that, as of the date of the filing of the application, the equipment is not "covered" equipment produced by entities identified on the Covered List.[146] The Commission proposed, further, that this attestation would encompass an attestation that no equipment, including any "component part," is comprised of "covered" equipment.[147] The Commission sought comment on whether such an attestation would be sufficient to implement the prohibition against authorization of covered equipment, the exact wording of the attestation, and the applicant's responsibility related to any changes in the Covered List.[148] In addition, the Commission asked whether it should require the applicant to provide, under section 2.1033, additional information (possibly including a "parts" list) that could help establish that the equipment is not "covered" in order to assist TCBs and the Commission in ensuring that applicants do not seek certification of "covered" equipment.[149] Finally, in the *NPRM*, the Commission proposed to direct OET, working with other bureaus and offices across the Commission (including PSHSB, WCB, IB, and EB), to develop pre-approval guidance or other guidance for applicants and TCBs in order to implement the prohibition on authorization of "covered" equipment.[150]

53. Some commenters offer support for the inclusion of an attestation requirement,[151] though several request that it be narrowly tailored.[152] Many commenters object in particular to the extension of the attestation (and prohibition) to include all component parts and urge the Commission not to require that applicants make attestations regarding such parts. They contend that such a requirement would be overly burdensome on applicants, difficult to implement (*e.g.*, the term is not clearly defined, applicants may have only limited knowledge of the product's origins or all manufacturers of equipment parts), impractical, and could create significant unintended supply chain issues.[153] NCTA asks that the

---

[145] We note that both existing and newly adopted rules use the term "certification" when referring to assurances made by applicants in addition to one of the two processes used for equipment authorization. To minimize confusion of terminology throughout the discussion in this item, we may use the term "attestation" when referring to such assurances, but for consistency in terminology in the rules themselves, we use the term "certification."

[146] *NPRM*, 36 FCC Rcd at 10600, para. 47. In the *NPRM*, the Commission discussed the then-current Covered List, which as discussed above identified five named entities and their subsidiaries and affiliates as producing "covered" equipment. *See, e.g.*, *NPRM*, 36 FCC Rcd at 10595, para. 37.

[147] *Id.* at 10600, para. 47.

[148] *Id.* at 10600, para. 47.

[149] *Id.* at 10600, para. 48.

[150] *Id.* at 10600-01, para. 49.

[151] *See*, *e.g.*, JVCKenwood Comments at 11; NCTA Comments at 14 (attestation requirements should be narrowly tailored); Motorola May 2, 2022 *Ex Parte* at 8 (supporting attestation requirement but noting clarity about what equipment is "covered" is necessary to prevent abuse; applicant also should be required to certify that it is not affiliated with or a subsidiary of a company with equipment on the Covered List); Hytera US Comments at 9 (proposes that the equipment authorization application process include submission of certain attestations to the TCB by the manufacturer).

[152] *See*, *e.g.*, CTIA Comments at 16-17 (requirement for attestation must be accompanied by clarity in the form of Commission guidance about the definitions of "telecommunications equipment," "video surveillance equipment," and component parts); *cf.* CTA Comments at 16-17 (any attestation requiring attestation on component parts would impose significant compliance burdens).

[153] *See*, *e.g.*, CTA Comments at 16 (applicants may lack the knowledge to confidently make attestations, likely under penalty of perjury, related to thus-far-undefined "component parts;" as a result, applicants may be dissuaded from developing new products that would need certification); CTIA Comments at 16 (new proposed attestation requirements also raise significant questions that are not addressed in the *NPRM*, particularly given uncertainties

(continued….)

Commission limit the scope of the attestation to "finished, fully assembled products."[154] Several commenters, including Motorola, CTIA, and CTA express concern that, without further clarification regarding equipment on the Covered List, an attestation could be overly burdensome and lead to abuse.[155] As for specific language to be included in the attestation, we received very few comments. Hytera US and JVCKenwood propose that we include several particular attestations to more clearly delineate the equipment's eligibility for authorization.[156] Motorola notes that the entities on the Covered List do not currently publicly disclose detailed information about their corporate relationships, including the names of their subsidiaries and affiliates, that the Commission should have visibility into these relationships, and that applicants should be required to attest that they are not affiliated with or a subsidiary of a company with equipment on the Covered List.[157]

54. We adopt a general attestation requirement in the form of a written and signed certification that the equipment is not prohibited from receiving an equipment authorization pursuant to new section 2.903.[158] Specifically, we revise section 2.911 to include a requirement that each applicant

about how the Commission will define and regulate component parts; in order to make accurate representations, applicants will need more clarity about what the Commission considers to be component parts); i-Pro Comments at 2 (requesting that, based upon the distinction between "equipment" as defined by the Commission's regulations and components that may be integrated into such equipment, the Commission does not revise its current regulations to require that any exempt devices (such as components) produced by an entity that has produced equipment included on the Covered List be subject to the Commission's certification rules and processes); NCTA Comments at 12-13 (requiring manufacturers to perform due diligence on every individual component of equipment or software they are considering in order to ensure that it is not on the covered list or prohibited from receiving an equipment authorization would impose considerable new burdens and costs that would likely be passed through to customers, significantly impacting equipment purchase and deployment decisions); NTCA Comments at 4 (network providers, especially small ones, have limited ability to identify the manufacturer of every component contained within any given piece of equipment and yet, these same providers are required to certify to the Commission that they do not have any covered equipment in their network).

[154] NCTA Comments at 12.

[155] CTIA Comments at 16; CTA Comments at 16; Motorola March 24, 2022 *Ex Parte* at 5.

[156] Specifically, Hytera proposes that section 2.911(d)(5) include the following attestation: whether the equipment is provided by an entity identified on the Covered List; whether, standing alone, the equipment provides fixed or mobile broadband connection speeds of at least 200 kbps; whether the equipment is capable of routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or services transmits or otherwise handles; whether the equipment is capable of causing the networks of a provider of advanced communications services to be disrupted remotely; whether the equipment has been deemed to pose an unacceptable risk to the national security of the United States or the security and safety of Unties States person by a specific determination made by an appropriate national security agency, as defined by section 1608 of the Act. Hytera US Comments at 12. JVCKenwood supports an attestation that the applicant and the equipment subject to the equipment authorization is not included on the most recent Covered List; that the applicant is not a "covered foreign country" as defined in the 2019 NDAA; that the applicant or declarant has not acquired its technology through unlawful means; and that the product subject to the application or declaration does not incorporate any unlawfully obtained technology. JVCKenwood Comments at 10-11.

[157] Motorola May 2, 2022 *Ex Parte* at 8 (applicant also should be required to certify that it is not affiliated with or a subsidiary of a company with equipment on the Covered List).

[158] We note such a certification requirement that the equipment is not prohibited from receiving an equipment authorization is similar in respects to a certification requirement placed on advanced communications service providers when submitting their annual reports identifying any "covered" communications equipment on the Covered List that they have purchased, rented, leased, or otherwise obtained after August 14, 2018. 47 CFR § 1.50007(a). The Commission already requires that each applicant provide a written and signed certification that all statements that it makes in its request are true and correct and that it complies with requirements of the Anti-Drug Abuse Act of 1988. 47 CFR §§ 2.911(d)(1)(2). We further note that with regard to the Federal agency implementation of its prohibition on procurement of "covered" equipment identified under section 889(f)(3) of the (continued….)

for equipment authorization in the certification process expressly provide a written and signed certification that, as of the date the applicant submits the required information to a TCB, the subject equipment is not prohibited from receiving an equipment authorization pursuant to section 2.903.[159]

55. We also will require that each applicant indicate, as part of this certification, whether it is an entity identified on the Covered List with respect to "covered" equipment.[160] We note that such entities on the Covered List could include entities specifically identified by name, as well as other associated entities, such as their subsidiaries and affiliates, and if so, then the applicant must indicate whether it is any such entity. We find that requiring submission of this additional information as part of the application for equipment certification will help ensure that prohibited "covered" equipment is not authorized. The rules that we are adopting to prohibit authorization of "covered" equipment rely in the first instance on the attestations by applicants at the beginning of the application process. Considering that applications for equipment certifications can be quite numerous,[161] we find that knowing whether an applicant for equipment certification is an entity identified on the Covered List is essential to the efficient and effective administration by the Commission and the TCBs of the statutory prohibition in our equipment authorization program. We agree with Motorola that transparency concerning the subsidiary or affiliate status of an applicant is important,[162] and this requirement will facilitate such transparency. While we note that indicating that the applicant is an entity on the Covered List does not mean that the subject equipment qualifies as "covered" equipment as such, such information nonetheless can potentially assist the TCBs, as well as the Commission in our oversight, and will be another feature that will be integral to ensuring that "covered" equipment in not authorized.[163] In sum, we find this requirement both reasonable and justified, particularly given the national security concerns relating preventing authorization of "covered" equipment[164] and the directive of Congress in the Secure Equipment Act.[165]

56. We note that the Covered List must be periodically updated,[166] which will likely result in periodic modifications as to the equipment or entities identified on the Covered List. Adopting a general attestation requirement, as opposed to a specific provision that directly relates to the equipment identified on the current Covered List, provides the flexibility for accommodating potential changes in the "covered" equipment on an updated Covered List. We recognize that there may be instances in which the Covered List is modified while an application for certification is pending. To ensure that we adequately address such changes to the Covered List, we adopt an additional requirement under section 2.911 specifying that, if the Covered List is modified after the date of the attestation but prior to grant of the

---

2019 NDAA, the offeror seeking to sell equipment to Federal agencies also are required to certify that their equipment is not "covered" equipment. *See* paragraph 13, above.

[159] *See* Rules, Appendix A, § 2.911(d)(5).

[160] In the *NPRM*, the Commission discussed the then-current Covered List, which as discussed above identified five named entities and their subsidiaries and affiliates as producing "covered" equipment. *See, e.g.*, *NPRM*, 36 FCC Rcd at 10595, para. 37. As discussed above, the current Covered List continues to identify these same five named entities and their subsidiaries and affiliates. *September 2022 Covered List Public Notice*, Appendix.

[161] We note, for instance, that more than 20,000 applications for certification were granted in 2021.

[162] Motorola May 2, 2022 *Ex Parte* at 8.

[163] We also note that if any applicant fails to disclose that it is an entity identified on the Covered List, this could provide grounds for revocation of any improperly granted authorization pursuant to streamlined procedures, as discussed below, or subject the entity to other enforcement measures.

[164] We note that, as discussed in section III.C.3, we also are requiring that to the extent that the Covered List identifies "covered" equipment as that produced by specifically named entities and certain unnamed associates (e.g., subsidiaries and affiliates), we require that the named entities provide the Commission information on their unnamed associates.

[165] Secure Equipment Act § 2(a)(2).

[166] *Id.* § 2(d).

authorization, then the applicant must provide a new written and signed certification that the subject equipment is not "covered" equipment identified on the Covered List as so amended.

57. Based on the record before us and the concerns raised, we find that any attestation that more broadly encompasses all "component parts" raises several issues that require additional consideration, and accordingly we seek further comment on those issues in the Further Notice of Proposed Rulemaking in this proceeding. Thus, we are not requiring, at this time, that the attestation specifically address individual component parts contained within the subject equipment, or provide any additional information in the application filed in accordance with section 2.1033.

58. We will require that applicants for equipment certification, when attesting that their equipment is not "covered," take into consideration the Commission's definitions and guidance regarding what constitutes "covered" equipment, as separately discussed below in more detail in this document.[167] Several commenters note the importance of clear guidance for purposes of the attestation requirement.[168] This guidance, which will be posted on the Commission's website, will be updated as appropriate to incorporate any further updates to the Covered List that affect "covered" equipment for purposes of the equipment authorization program, and will provide additional clarity regarding the requisite attestation. Attestations by each applicant that the subject equipment is not prohibited from receiving an equipment authorization must be true and accurate. As discussed below, in order to protect against abuse of the application process that relies on this attestation, we also are adopting new procedures for revoking equipment certifications for false statements or representations made by any applicant in its application for certification regarding "covered" equipment.[169]

b. Agent for service of process located in the United States

59. In the *NPRM*, the Commission sought comment on actions that it should take that would better ensure that equipment certification applicants and grantees comply with the requirements proposed in the *NPRM*. In particular, the Commission proposed requiring that the party responsible for compliance with the applicable requirements concerning certified equipment have a party located within the United States that would be responsible for compliance, akin to the current requirement applicable for equipment authorized through the SDoC process.[170] The Commission also asked whether it should require the applicant for an equipment certification to identify an agent for service of process that must be located within the United States.[171] Finally, the Commission sought comment on how much additional burden such requirements would place on the applicant and whether similar requirements should be placed on grantees of existing equipment authorizations.[172]

60. The Commission received little comment on these issues. Regarding the proposal that the party responsible for compliance of certified equipment be located within the United States, only Hytera US commented, supporting the identification of a U.S.-based responsible party.[173] As for the agent for service of process issue, only 5G Americas commented, stating that it "does not object" to requiring existing authorized equipment providers to provide a local contact for service of process or inquiries from the Commission.[174]

---

[167] *See* Section III.C.5, below.

[168] *See, e.g.*, CTIA Comments at 16-17; CTA Comments at 16; NTCA Comments at 4-5; Motorola March 24, 2022 *Ex Parte* at 5-6.

[169] *See* Section III.B.6 below; 47 CFR § 2.939.

[170] *NPRM*, 36 FCC Rcd at 10603, para. 54.

[171] *Id.* at 10603, para. 54.

[172] *Id.* at 10603, para. 54.

[173] Hytera US Comments at 13.

[174] *See* 5G Americas Comments at 3.

61. We continue to believe that it is important for the Commission to facilitate enforcement of our rules, and our actions in this proceeding to prohibit future authorization of "covered" equipment that poses an unacceptable risk to national security underscore the need for effective enforcement of applicable rules associated with certified equipment. For many certified devices that are imported to and marketed in the United States the grantees of the associated equipment authorizations are located outside of the United States. It is not always easy to communicate effectively with grantees, particularly foreign-based grantees, in order to engage in relevant inquiries, determine compliance, or even enforce our rules where appropriate. Accordingly, we believe it important that we have a reliable and effective means by which we can readily identify and contact a representative of the grantee of an FCC equipment certification.

62. Accordingly, in this Report and Order, we are adopting a requirement that each applicant for equipment certification designate a contact located in the United States for purposes of acting as its agent for service of process, regardless of whether the applicant is a domestic or foreign entity.[175] We believe that this requirement is straightforward, easy to implement, and should not place much of a burden on applicants seeking equipment authorization. However, as for the proposal to require that, for equipment certification, the party responsible for compliance be located in the United States, we find that defining specific requirements that the Commission should adopt and implementing them within our processes raise more complicated issues. Thus, we further conclude that the Commission would benefit from further consideration of these issues in the Further Notice of Proposed Rulemaking portion of this item.[176]

63. An agent for service of process traditionally holds the obligation to accept the service of process and other documents on behalf of the party chiefly responsible, and to swiftly and dutifully deliver them to that party. Service of process includes, but is not limited to, delivery of any correspondence, notices, orders, decisions, and requirements of administrative, legal, or judicial process related to Commission proceedings.[177] The rule we are adopting reflects other well-established service of process requirements in the Commission rules.[178]

64. For purposes of implementing this requirement, we revise our rules to require that the applicant for equipment certification include with its application for certification a written certification identifying the agent for service of process by name, U.S. physical address, U.S. mailing address (if different), e-mail address, and telephone number.[179] An applicant that is located in the United States may designate itself as the agent for service of process. The attachment designating the agent for service of process must include a statement, signed by both the applicant and its designated agent for service of

---

[175] Appendix A, § 2.911(d)(6).

[176] *See* Further Notice of Proposed Rulemaking below.

[177] In this context, legal or judicial proceedings extend to any proceedings needed to enforce a Commission order. *See*, *e.g.*, 47 U.S.C. §§ 401, 504.

[178] *See, e.g.*, 47 CFR §§ 1.5 (requiring each licensee to provide a mailing address, and each Wireless licensee to also provide an e-mail address, which will be used by the Commission for service of process and correspondence); 1.47(h) (requiring international section 214 authorization holders to designate a U.S. citizen or lawful U.S. resident, located in the District of Columbia, upon whom service may be made); 64.2115(a)(2) (registration of intermediate providers of rural call completion requires provision of designated agent for service of process); 68.321 (requiring the responsible party for Supplier's Declaration of Conformity equipment that operates under part 68 to "designate an agent for service of process that is physically located in the United States"); *see also* 47 U.S.C. § 413 (requiring every carrier to designate an agent in the District of Columbia that is responsible for accepting service on its behalf).

[179] As outlined *supra*, section III.B.2 (Certification rules and procedures), a TCB reviews each application for equipment certification to ensure that it meets the Commission's requirements. *See* 47 CFR § 2.911(a). Section 2.917 gives the TCB the ability to dismiss an incomplete application. *See id.* § 2.917(a). Therefore, under today's rule change, a TCB must dismiss an application if that application omits the identification of the U.S.-based agent for service of process.

process, if different from the applicant, acknowledging the applicant's consent to accept service of process in the United States at the physical mailing address, U.S. mailing address (if different), and e-mail address of its designated agent,[180] as well as the agent's acceptance of its obligation. Requiring that the agent expressly consent to service within the United States will enable the Commission to efficiently carry out its enforcement duties, and if the grantee is foreign-based, will facilitate enforcement without the need to resort to unwieldy procedures that may otherwise apply under international law.[181] The written certification must also include the applicant's acknowledgment that the designation of the agent must remain in effect for no less than one year after the grantee has terminated all marketing and importing of the associated certified equipment within the United States or the conclusion of any Commission-related administrative or judicial proceeding involving the equipment, whichever is later. In line with existing Commission rules, service is deemed to be complete when the document is sent to the U.S. physical address, U.S. mailing address (if different), or e-mail address of the U.S.-based agent for service of process.[182] While, as discussed in the *NPRM*, the Commission sought comment on whether to apply such a requirement for an agent for service of process located in the United States to equipment already authorized pursuant to the certification process, we decline to do so in this Report and Order unless there is a change in the name or address of the grantee or the grantee modifies the authorized equipment, as discussed immediately below.

c. Modification of equipment, including permissive changes

65. In the *NPRM*, the Commission sought comment on possible revisions to the part 2 rules to ensure that equipment users will not make modifications to existing equipment that would involve replacement with "covered" equipment.[183] In particular, the Commission asked whether it should revise section 2.932 regarding modifications to equipment (e.g., changes in the design, circuitry, or construction of the device) or the section 2.1043 provisions concerning changes to certified equipment, such as "permissive changes."[184]

66. We find that, in order to fully implement our newly adopted prohibition on authorization of "covered" equipment we must also revise section 2.932 concerning modification of equipment. A modification to authorized equipment could result in the later identification of that equipment as "covered." we cannot allow the continued authorization of modified equipment if, at the time of such modification, the equipment is "covered" equipment on the Covered List. Accordingly, we adopt revisions to section 2.932 to require, similar to the revised provisions of section 2.911, that all applications or requests to modify already certified equipment include a written and signed certification that the equipment is not prohibited from receiving an equipment authorization pursuant to section 2.903.

---

[180] Entities that do business with the Commission are required to provide a valid e-mail address when they register for an FCC Registration Number (FRN) in the Commission Registration System (CORES). *See* 47 CFR § 1.8002(b)(1). Applicants for an equipment certification must obtain an FRN, and therefore parties responsible for certified equipment are currently required to provide the Commission with an e-mail address. We expressly provide here that this e-mail must be included in the application for certification. *See Amendment of Part 1 of the Commission's Rules, Concerning Practice and Procedure, Amendment Of Cores Registration System*, Report and Order, 36 FCC Rcd 10773 (2021) (adopting an e-mail requirement for the Commission's CORES system after noting the wide availability of free or low-cost Internet access). *Office of Managing Director will Decommission Legacy Commission Registration System on July 15, 2022*, MD Docket 10-234, Public Notice, DA 22-508, 2022 WL 1786500 (OMD May 27, 2022) (explaining that Legacy CORES will be replaced by CORES 2).

[181] Treaty obligations may require complex service of process procedures that delay enforcement, but such procedures are inapplicable when service is made on a domestic agent. *See Volkswagen v. Schlunk*, 486 U.S. 694, 707 (1997).

[182] *See* 47 CFR § 1.47(f) ("Service by mail is complete upon mailing. Service by email is complete upon sending to the e-mail address listed in the ULS for a particular license, application, or filing.").

[183] *NPRM*, 36 FCC Rcd at 10602, para.52.

[184] *Id.* at 10602, para. 52; 47 CFR §§ 2.932, 2.104.

We also require an affirmative or negative statement as to whether the applicant is identified on the Covered List, as well as the written and signed certifications required under section 2.911(d)(6) regarding an agent for service of process within the U.S. Similarly, we also adopt the same provisions for requests for Class II and III permissive changes pursuant to section 2.1043.[185] We find that these revisions are sufficient to prevent modified equipment from maintaining authorization when such modifications occur at a time after which such equipment has been identified as posing a risk and thereby appearing on the Covered List.

d. Requirements that grantees update certain changes following grant of certification

67. Considering that section 2.929 includes provisions regarding changes in the name, address, ownership, or control of the grantee of an equipment authorization, in the *NPRM* the Commission also asked whether revisions were appropriate to that rule, consistent with the goals of this proceeding.[186] Section 2.929 sets forth the requirements that the grantee of an equipment certification must maintain accurate, up-to-date contact information on file with the Commission: "[w]henever there is a change in the name and/or address of the grantee of certification, notice of such change(s) shall be submitted to the Commission via the Internet at https://apps.fcc.gov/eas within 30 days after the grantee starts using the new name and/or address."[187] The grantee also must report the assignment, exchange, or certain transactions affecting the grantee (e.g., transfer of control or sale to another company, mergers, and/or manufacturing rights), irrespective of whether the Commission requires a new application for certification.[188] The current rule also permits a grantee to license or otherwise authorize a second party to manufacture the equipment.[189] We did not receive comments on updating section 2.929.

68. We adopt revisions to section 2.929 in order to ensure that certain post-authorization changes do not result in that equipment becoming "covered" equipment that pose an unacceptable risk to national security. We find that certain changes in the name, address, ownership, or control of the grantee of an equipment authorization could result in previously authorized equipment being produced by an entity identified on the Covered List as producing "covered" equipment, thus resulting in the equipment becoming "covered" equipment. Accordingly, we revise our requirements in section 2.929 to ensure that a grantee cannot circumvent our prohibition on authorization of equipment on the Covered List by transferring ownership or control, or licensing or otherwise authorizing a second party to manufacture the equipment associated with the grant of the equipment authorization. Specifically, we revise section 2.929 to prohibit the grantee of an equipment authorization from licensing or otherwise authorizing a second party to manufacture the equipment covered by the grant of the equipment authorization if such licensing or authorization would result in the equipment falling within the scope of "covered" equipment. We further adopt a requirement that notice of any change in the name or address of the grantee of certification, or transactions affecting the grantee (such as a transfer of control or sale to another company, mergers, or transfer of manufacturing rights), include provisions similar to the revised provisions of section 2.911. Specifically, we require that the notice include a written and signed certification that as of the date of the filing of such notice, the equipment to which the change applies is not prohibited from receiving an equipment authorization pursuant to section 2.903. We also require that the notice include an affirmative or negative statement as to whether the grantee is identified on the

[185] Class 2 and Class 3 permissive changes are significant enough that they require submission of test results. *See* 47 CFR § 2.1043(b)(2)-(3). Therefore the requested certification that the equipment is not on the Covered List and an attachment identifying the agent for service of process would be submitted along with the test results. Because no filings are currently requested for the less significant Class 1 permissive changes, *see* 47 CFR § 2.1043(b)(1)), this requirement would not apply.

[186] *NPRM*, 36 FCC Rcd at 10602, para. 52; 47 CFR § 2.929.

[187] 47 CFR § 2.929(c).

[188] *See id*. § 2.929(a) and (d).

[189] *Id.* § 2.929(b).

Covered List (e.g., is subsidiary or affiliate of an entity named on the Covered List as producing "covered" equipment.

69. We also revise section 2.929 to help ensure compliance with our effective service of process requirement added to section 2.1033, described above. For the same reasons that we require a U.S.-based agent for service of process for applicants, we will require that the grantee maintain an agent for service of process that is located in the United States. Therefore, we add to section 2.929 the requirement that grantees must report any change to the information of the designated U.S.-based agent for service of process in updating the information on file with the Commission along with the written and signed certifications required under new section 2.911(d)(7).

e. Other issues

70. *Conforming edits in part 2.* We make several conforming edits in our part 2 rules to reflect the requirements that we are adopting in this Report and Order. Several part 2 rules are revised, as appropriate to reflect that the requirements for equipment authorization now include the responsibility to comply with non-technical requirements such as the Covered List prohibitions.[190] We note here that we also adopt in section 2.1033 the provisions adopted 2.911(d) to clarify that the required information must be provided with the application for certification.

71. *Other issues raised in the NPRM.* In the *NPRM*, the Commission sought comment on other possible steps that it should consider that would affect its certification rules, such as actions that could be taken following grant of an equipment authorization that might be helpful in enforcing the prohibition on authorization of "covered" equipment. These included whether the Commission should consider adopting any post-grant review procedures following the grant of an equipment authorization,[191] or any revisions or clarifications concerning "post-market surveillance" activities with respect to products that have been certified.[192] In the few comments we received on these issues, most opposed any changes,[193] and we are not at this time adopting any revisions or clarifications to the Commission's rules on these issues. We do, however, think they merit further consideration, particularly now that we are adopting a specific set of rules and procedures prohibiting authorization of "covered" equipment. Accordingly, we do seek further comment in the Further Notice portion of this item, requesting comment in light of the rule revisions that we are adopting herein.

3. Supplier's Declaration of Conformity (SDoC) rules and procedures

72. In the *NPRM*, the Commission proposed that any equipment produced by any of the entities (or their respective subsidiaries or affiliates) that produce covered equipment, as specified on the Covered List, would no longer be authorized pursuant to the Commission's SDoC processes, and that the equipment of any of these entities would be subject to the Commission's certification process. Under this approach, responsible parties would be prohibited altogether from relying on authorization using the SDoC process with respect to any equipment produced or provided by these entities (or their respective subsidiaries or affiliates), as such equipment could not be authorized utilizing the SDoC process.[194] The Commission sought to ensure consistent application of its prohibition on further authorization of any "covered" equipment by requiring a single process, the certification process, which involves more active Commission oversight than the SDoC process for equipment produced by any entity identified on the

[190] *See, e.g.*, *id.* §§ 2.901(a), 2.909(a).

[191] *NPRM*, 36 FCC Rcd at 10601, para. 50 (noting that current rules permit the TCB or Commission to set aside a grant of certification within 30 days of the grant if determined that such authorization does not comply with applicable requirements or is not in the public interest).

[192] *Id.* at 10601, para. 51; *see* 47 CFR § 2.962(g).

[193] We note that the Commission received few comments on some of these issues.

[194] *NPRM*, 36 FCC Rcd at 10604-05, para. 59.

Covered List as producing "covered" equipment.[195] The Commission also invited comment on the specific information that should be included in the SDoC compliance statement that would ensure that responsible parties do not use the SDoC process for equipment produced by entities identified on the Covered List as producing "covered" equipment.[196]

73. As discussed in the *NPRM*, the SDoC procedures, which are available for specific equipment generally considered to have reduced potential to cause harmful RF interference, permits equipment to be authorized through reliance on the responsible party's self-declaration that the equipment complies with the pertinent Commission requirements.[197] Accordingly, the SDoC process differs significantly from the certification process, and does not involve the more active and transparent oversight of the certification process.[198] Many devices eligible for an SDoC authorization do not contain a radio transmitter and include only digital circuitry (e.g., computer peripherals; microwave ovens; industrial, scientific, and medical (ISM) equipment; switching power supplies; light-emitting diode (LED) light bulbs; radio receivers; and TV interface devices), although an SDoC authorization is also permitted for certain transmitters used in licensed services.[199] As the Commission noted, under existing rules the use of SDoC procedures are "optional," as each responsible party for an SDOC-eligible device could choose to obtain equipment authorization using either certification or SDoC procedures.[200]

74. For each particular RF device, the completion of the SDoC process signifies that the responsible party affirms that the necessary measurements have been made, or other procedures that have been found acceptable to the Commission have been completed, to ensure that the particular equipment complies with the applicable requirements.[201] As set forth in our rules, the responsible party may be the equipment manufacturer, the assembler (if the equipment is assembled from individual component parts and the resulting system is subject to authorization), or the importer (if the equipment by itself or the

---

[195] *Id.* at 10605, para. 59.

[196] *Id.* at 10605, 10605-06; paras. 60, 62.

[197] *Id.* at 10604, para. 57.

[198] *Id.* at 10604, para. 57. Among other things, certification of equipment requires use of a third-party FCC-recognized Telecommunication Certification Body, based on an evaluation of supporting documentation and test data contained in an application submitted by the responsible party (*e.g.*, the manufacturer or importer) to the TCB. In addition, compliance testing for certification must be performed by an FCC-recognized accredited testing laboratory. Further, unlike equipment authorized through the SDoC process, the technical parameters and descriptive information for all certified equipment are posted on a Commission-maintained public database (https://www.fcc.gov/oet/ea/fccid). *See* 47 CFR §§ 2.907 *et seq*.

[199] *See* Supplier's Declaration of Conformity Guidance, FCC Office of Engineering and Technology Laboratory Division, December 20, 2019, at 2; document is available at https://apps.fcc.gov/kdb/GetAttachment.html?id=cPjFB7kIR2TMlwiHUNAbvA%3D%3D&desc=896810%20D01%20SDoC%20v02.pdf&tracking_number=203240. [Check cite, parentheses may be missing.] More specifically, the types of equipment that may be processed pursuant to the SDoC procedure include fixed microwave transmitters (e.g., point-to-point or multipoint transmitter links as well as some links used by carriers and cable operators) authorized under part 101, broadcast TV transmitters authorized under parts 73 and 74, certain ship earth station transmitters authorized under part 80 (Maritime), some emergency locator transmitters authorized under part 87 (Aviation), and private land mobile radio services equipment and equipment associated with special services such as global maritime distress and safety system, aircraft locating beacons, ocean buoys), certain unlicensed equipment (e.g., business routers, firewalls, internet routers, internet appliances, wired surveillance cameras, business servers, workstations, laptops, almost all enterprise network equipment, computers, alarm clocks) that includes digital circuitry (but no radio transmitters) authorized under part 15, certain ISM equipment (e.g., those that use RF energy for heating or producing work) authorized under part 18.

[200] 47 CFR § 2.906(c).

[201] *See id.* §§ 2.906 ("Supplier's Declaration of Conformity"); 2.9391 ("Responsibilities"); 2.938 ("Retention of records"); 2.945 ("Submission of equipment for testing and equipment records"); 2.1071-1077 ("Supplier's Declaration of Conformity").

assembled system is subject to authorization),[202] or, under certain circumstances, retailers or parties performing equipment modification.[203] For devices subject to SDoC, the information the responsible party must keep on file includes a compliance statement that lists a U.S.-based responsible party.[204] The SDoC process is "streamlined" in the sense that, unlike the certification process, it does not require submission of applicable information to a Commission-recognized TCB or the use of an FCC-recognized accredited testing laboratory.[205] However, the Commission can specifically request that a responsible party provide compliance documentation or device samples as necessary.[206]

a. Prohibition on use of SDoC process for entities producing "covered" equipment on the Covered List

75. In proposing in the *NPRM* that equipment produced by any of the entities (or their respective subsidiaries or affiliates) identified on the Covered List as producing "covered" equipment would no longer be authorized pursuant to the Commission's SDoC process, the Commission sought to ensure consistent application of its proposed prohibition on authorization of "covered" equipment. The Commission contend that by shifting such equipment to the certification process, which involves more active oversight, including proactively providing guidance when working directly with TCBs prior to any equipment authorization, it would facilitate more effective post-market surveillance as appropriate.[207] Because the Commission does not have direct involvement in the SDoC process (e.g., nothing is filed with or recorded by the Commission), that process presents significant additional challenges to ensure that covered equipment that might otherwise be eligible for the SDoC process does not make its way into the U.S. market.

76. Several commenting parties express reservations about the Commission's proposed SDoC approach, and Hikvision USA and Dahua USA expressly oppose it altogether.[208] Specifically, CTA and NCTA commenters express concern that the proposal is overly broad and could present compliance challenges for equipment manufacturers, many of whom rely on this streamlined process, and would require use of the more burdensome and time-consuming certification process.[209] ITI raises concerns that the SDoC proposal could capture a range of equipment not contemplated by Congress or the other expert agencies tasked with determining which equipment should be included on the Covered List.[210] Dahua USA contends that the Commission lacks statutory authority to refuse or restrict authorization of equipment based solely on the identity of the manufacturer. Dahua USA also maintains that enactment of the Secure Equipment Act does not change the status of its equipment because that

---

[202] *Id.* § 2.909(b)(1)-(2).

[203] *Id.* § 2.909(b)(3)-(4).

[204] *Id.* § 2.1077(a)(3).

[205] For example, while our rules require that the equipment authorized under the SDoC procedure must include a unique identifier, as discussed above, the equipment is not listed in a Commission equipment authorization database. 47 CFR § 2.1074. We observe that the format of "unique identifier" is at the responsible party's discretion and has no correlation to a Commission-established FCC ID.

[206] The responsible party is required to retain records on the equipment that demonstrates compliance with the Commission's requirements for that equipment. 47 CFR § 2.938. The Commission may request these records and request equipment samples 47 CFR §§ 2.906(a), 2.945(b) & (c).

[207] *NPRM*, 36 FCC Rcd at 10604-05, para. 59.

[208] *See, e.g.*, Hikvision USA Feb. 23, 2022 *Ex Parte* at 4 (excluding Hikvision equipment from the SDoC process would impose substantial and unjustifiable costs on consumers seeking to replace or purchase new equipment); Dahua USA Comments at 15; Dahua USA Reply Comments at 2 (Dahua USA notes, however, that it is willing to supply the Commission with information on any SDoC-authorized equipment).

[209] *See, e.g.*, CTA Comments at 19; NCTA Comments at 14.

[210] ITI Comments at 11-12.

enactment directs the Commission to deny authorization only to "covered" equipment. It further asserts that the Commission's proposed rules lack a rational basis absent requisite statutory grounding, and that logic does not support subjecting entities with only some "covered" equipment on the Covered List to a more onerous certification process for all equipment.[211]

77. Other commenters, however, generally agree with the Commission's approach to ensuring that prohibited equipment is not authorized. Brunner specifically applauds the Commission for proposing to add new section 2.903 to its rules to prohibit covered equipment from being authorized either through the certification or SDoC processes.[212] Motorola agrees with the Commission's proposed approach that only the certification process, and not the SDoC process, be available for authorizing equipment produced by entities named on the Covered List, contending that will help ensure needed transparency.[213] Moreover, JVCKenwood argues that the Commission is obligated, pursuant to existing legislation and Executive Orders, to prohibit the authorization of equipment manufactured by entities on the Covered List; and to preclude the further marketing and deployment of "covered" equipment that has in the past been certified or authorized via the SDoC process. JVCKenwood recommends that the Commission scrutinize certification applications and products subject to SDoC that are manufactured by entities who have been adjudicated to have – with respect to the manufacture, marketing, or sale of their telecommunications products – perpetrated serious wrongdoing.[214]

78. We are not persuaded by opponents of our proposal who assert that it is unnecessarily burdensome. Entities following either the certification or the SDoC process must both prove compliance with FCC rules through testing and supporting documentation.[215] Given that information on equipment authorized via the SDoC process is not readily transparent to the Commission, the certification process provides the Commission with the necessary oversight to ensure that we are achieving our goals in this proceeding to prohibit authorization of equipment that poses an unacceptable risk, as required by the Secure Equipment Act, and will help prevent "covered" equipment from improper authorization through the SDoC process in the first place. We find that it is appropriate and reasonable to foreclose the SDoC process to equipment produced by any entity identified on the Covered List as producing "covered" equipment and require equipment authorization through the certification process. We adopt as proposed a rule prohibiting any of the entities identified on the Covered List as producing "covered" equipment from using the SDoC process to authorize any equipment – not just "covered" equipment identified on the Covered List. Thus, any equipment eligible for equipment authorization that is produced by any entities so identified on the Covered List must be processed pursuant to the Commission's certification process, regardless of any Commission rule that would otherwise permit use of the SDoC process.

79. As explained in the *NPRM*, we believe that requiring use of only one process by entities that have already been determined to produce "covered" equipment will serve the important goal of ensuring consistent application of our newly adopted prohibition on further authorization of any "covered" equipment, while also providing for more active oversight. Considering the importance of prohibiting equipment for devices that pose an unacceptable risk to national security, and that this is the Commission's first foray into implementing rules and procedures that require effective identification and prohibition of equipment that poses an unacceptable risk to national security, we find this approach at this time is consistent with the public interest.[216] We note that, as the Commission, industry, and

[211] Dahua USA Jan. 4, 2022 *Ex Parte* at 12-13.

[212] Brunner Comments at 17.

[213] Motorola Aug. 10, 2022 *Ex Parte* at 6 (rejecting Hikvision USA's proposed approach of permitting continue use of the SDoC process so long as the equipment authorized under this process is reported to the Commission).

[214] JVCKenwood Comments at 2.

[215] *See* 47 CFR §§ 2.906, 2.907.

[216] *NPRM*, 36 FCC Rcd at 10604-05, para. 59.

manufacturers gain more experience over time on the effectiveness of its SDoC procedures concerning "covered" equipment, the Commission may revisit this process.

b. Attestation requirement

80. In the *NPRM*, the Commission sought comment on what information should be included in the SDoC compliance statement to ensure that responsible parties do not use the SDoC process to authorize "covered" equipment.[217] In the Commission's view, this compliance statement would need to be sufficiently complete to ensure that a responsible party exercises the necessary diligence to confirm that equipment that is subject to the SDoC process is not "covered" equipment for purposes of equipment authorization. Further, the Commission indicated that this compliance statement should be crafted in such a manner as to assist responsible parties in ensuring authorization is achieved through the appropriate process by identifying equipment produced by any entity identified on the Covered List as producing "covered" equipment, which can no longer be authorized through the SDoC process. This statement would also ensure that responsible parties are held accountable, by their compliance statement, for any misrepresentations or violation of the prohibition that we are adopting here.[218]

81. We received few comments specifically regarding our proposal to require a compliance statement attestation affirming that the equipment is not "covered" equipment included on the Covered List. NCTA comments that attestation requirements for SDoC rules should be narrowly tailored to avoid creating compliance challenges for all equipment manufacturers and others seeking equipment authorization.[219] JVCKenwood suggests that the Commission require not only an affirmative statement that neither the applicant nor the equipment is included on the Covered List, but also additional attestations outside of the scope of "covered" equipment identified on the Covered List (e.g., that the applicant is not a "covered foreign country" as defined by the 2019 NDAA, that the applicant did not acquire the technology through unlawful means, and that the product does not incorporate any unlawfully-obtained technology.[220]

82. As we did for the certification process, we adopt a general attestation requirement in the form of a written and signed certification that the equipment is not produced by any entity identified on the Covered List as producing "covered" equipment, pursuant to section 1.50002 of the Commission's rules.[221] Specifically, we revise section 2.938 to include a requirement that the responsible party maintain record of a written and signed certification that, as of the date of first importation or marketing, the equipment for which the responsible party maintains Supplier's Declaration of Conformity is not produced by any entity that is identified on the Covered List as producing "covered" equipment.[222] We find that the existing SDoC operational framework, in which the responsible party declares that the equipment complies with the pertinent Commission requirements, in concert with an explicit attestation by each responsible party completing the SDoC process that the subject equipment is not produced by any

[217] *Id.* at 10605, para. 60.

[218] *Id.* at 10605, para. 60.

[219] NCTA Comments at 14.

[220] JVCKenwood Comments at 11.

[221] We note such a certification requirement that the equipment is "not" covered is similar in respects to a certification requirement placed on advanced communications service providers when submitting their annual reports identifying any "covered" communications equipment on the Covered List that they have purchased, rented, leased, or otherwise obtained after August 14, 2018. 47 CFR § 1.50007(a). The Commission already requires that each applicant provide a written and signed certification that all statements that it makes in its request are true and correct and that it complies with requirements of the Anti-Drug Abuse Act of 1988. 47 CFR §§ 2.911(d)(1)(2). We further note that with regard to the Federal agency implementation of its prohibition on procurement of "covered" equipment identified under section 889(f)(3) of the 2019 NDAA, the offeror seeking to sell equipment to Federal agencies also are required to certify that their equipment is not "covered" equipment. *See* paragraph 13, *supra.*

[222] *See* Appendix A, § 2.938(b).

entity identified on the Covered List as producing "covered" equipment, pursuant to section 1.50002 of the Commission's rules, should be sufficient to render unlikely the possibility that equipment required to be processed through our certification procedures will instead be erroneously processed under our SDoC procedure. We find that JVCKenwood's suggestions that the attestation include other considerations beyond whether the equipment is "covered" (e.g., an attestation that the equipment was not unlawfully acquired) are beyond the scope of the Commission's proposal in this proceeding.

83. The required attestation by the responsible party for each device authorized under SDoC is similar to that required of applicants in the certification process.[223] As with the attestation included in a certification application, we will require a simple attestation here that the equipment is not produced by an entity identified on the Covered List as producing "covered" equipment, pursuant to section 1.50002 of the Commission's rules. We do not believe that such a requirement will present an undue burden when weighed against the potential security risks described by Congress nor should it present any delay in the authorizing equipment through the SDoC process. Such an attestation will also provide a mechanism for the Commission to, as needed, verify the origin of equipment authorized by SDoC and ensure accountability for a responsible party dealing with equipment provided by entities on the Covered List. We expect that these measures will be sufficient to deter responsible parties from seeking the SDoC process for authorization of equipment on the Covered List, and we will rely on the Commission's enforcement procedures to ensure compliance. We note that our current rules require that the SDoC responsible party be located within the United States, and that the party's name, address, and telephone number or Internet contact information be included in the compliance information that is provided with authorized equipment, and we do not alter this requirement.[224]

c. Enforcement

84. In the *NPRM*, the Commission also asked several questions relating to enforcement of the SDoC prohibitions and related requirements. In this regard, the Commission noted its existing authority to request equipment samples and compliance information,[225] and asked questions about the circumstances that would warrant Commission requests and what information would be useful in proving/disproving such compliance.[226] We received no comments or suggestions on how the Commission should approach these issues.

85. As noted in the *NPRM*, the Commission already has the authority to request that the responsible party provide information regarding any equipment that has been authorized through the SDoC procedures.[227] Accordingly, we will exercise our oversight, as appropriate, by requesting that the

[223] *See* Appendix A, § 2.911.

[224] 47 CFR § 2.1077(a)(3).

[225] *NPRM*, 36 FCC Rcd at 10605-06, para. 62 n.187. *See* 47 CFR §§ 2.906(a); 2.945(b)(1) (Commission may request that the responsible party or any other party marketing the equipment submit a sample); 2.945(c) (upon request by the Commission, each responsible party shall submit copies of records required under the Commission's rules, including – the original design drawings and specification; procedures for inspection and testing; test results; actual date of testing; name of the test lab, company, or individual performing the testing; description of the equipment; and/or the "compliance information" required under the rules). *See* 47 CFR § 2.1077 (Compliance information). The Commission's rules include procedures wherein the Commission can suspend action on application or require forfeiture. *See* 47 CFR §§ 2.945(b)(5), 2.945(c). Upon request by the Commission, each responsible party must make its manufacturing plant and facilities available for inspection. 47 CFR § 2.945(d).

[226] *NPRM*, 36 FCC Rcd at 10605-06, para. 62.

[227] 47 CFR §§ 2.906(a); 2.945(b)(1) (Commission may request that the responsible party or any other party marketing the equipment submit a sample); 2.945(c) (upon request by the Commission, each responsible party shall submit copies of records required under the Commission's rules, including – the original design drawings and specification; procedures for inspection and testing; test results; actual date of testing; name of the test lab, company, or individual performing the testing; description of the equipment; and/or the "compliance information" required under the rules). *See* 47 CFR § 2.1077 (Compliance information). The Commission's rules include procedures (continued….)

responsible party provide to us relevant information – e.g., an equipment sample, representative data demonstrating compliance, and the compliance statement itself, including the attestation (in the form of a written and signed certification) required by this action, and any information necessary to assess the validity of that attestation – regarding any equipment that we deem requires confirmation of its compliance with our rules. As with equipment authorized through our certification process, we will take any available enforcement action to ensure that equipment identified on the Covered List does not receive equipment authorization and to hold accountable any entity that fails to accurately attest that any equipment for which the seek authorization is "covered" equipment. We also will work with our federal partners to identify and block the importation of "covered" equipment that is placed on the Covered List and is prohibited from equipment authorization pursuant to the rules adopted in this Report and Order.

86. Finally, in light of the newly established SDoC rules and procedures to prohibit authorization of "covered" equipment, we invite further comment in the Further Notice of Proposed Rulemaking on other actions the Commission should consider when carrying out its responsibilities to ensure compliance with the prohibitions on authorization of "covered" equipment that we are adopting in this Report and Order.

4. Importation and marketing rules

87. As the Commission noted in the *NPRM*, if it adopted its proposal to revise the Commission's subpart J equipment authorization rules to prohibit any further authorization of covered equipment through the certification or SDoC processes, this decision also would prohibit the marketing of such equipment under subpart I of the Commission's part 2 rules (Marketing of Radio-Frequency Devices)[228] and importation of equipment under subpart K (Importation of Devices Capable of Causing Harmful Interference) of our part 2 rules.[229] In the *NPRM*, we sought comment on whether to revise or provide clarification with regard to how our proposal to prohibit authorizing covered equipment would affect the Commission's rules in either subpart I or subpart K. Specifically, we asked whether the general prohibition we proposed for equipment subject to certification and SDoC made any changes to subparts I or K unnecessary and, if not, what changes were needed to our rules in those subparts.[230]

88. We affirm the conclusion that revising the general equipment authorization provisions in subpart J also effectively prohibits the marketing and importation of "covered" equipment prohibited from authorization under the equipment authorization program. Section 2.803(b) only permits persons to market RF devices that are subject to authorization under either the certification or SDoC process, as set forth in the Commission's subpart J rules, once those devices have been authorized,[231] unless an exception applies.[232] Similarly, our revisions in this proceeding to the equipment authorization process in subpart J, above, also prohibits importing or marketing of covered equipment if it is subject to authorization through either the certification or SDoC process in subpart J and has not been authorized, per sections 2.1201(a) and 2.1204(a).[233]

89. Huawei Cos. argue that the Commission's equipment authorization rules were adopted pursuant to express statutory provisions that deal with technical issues, and none authorize the

---

wherein the Commission can suspend action on application or require forfeiture. *See* 47 CFR § 2.945(b)(5), (c). Upon request by the Commission, each responsible party must make its manufacturing plant and facilities available for inspection. 47 CFR § 2.945(d).

[228] 47 CFR §§ 2.801 *et seq.*

[229] *Id.* §§ 2.1201 *et seq.*; *see NPRM*, 36 FCC Rcd at 10596-97, para. 42.

[230] *Id.* at 10598, para. 42.

[231] 47 CFR § 2.803(b) (concerning part 2 subpart I rules, "Marketing of Radio-Frequency Devices").

[232] *Id.* § 2.803(c) (listing the exceptions to the general rule of section 2.803(b)).

[233] *Id.* §§ 2.1201(a), 2.1204(a) (concerning part 2, subpart K rules, "Importation of Devices Capable of Causing Harmful Interference").

Commission to prohibit the importation, marketing, or sale of a company's products en masse without regard to the technical characteristics of a particular product (with one exception specifically required by statute and premised on a prior criminal conviction of the registrant).[234] Dahua USA contends that a significant amount of its equipment imported, marketed, sold, and used in the United States is used in a closed network environment entirely disconnected from the broader public network, such that prohibiting its equipment would not generate any increased security benefits to communications networks.[235]

90. CTA recommends that we exempt from prohibition the continued importation and use of equipment produced by entities on the Covered List for research, development, and testing purposes.[236] CTA maintains that the importation of such equipment for these limited purposes would further innovation without posing any great risk to national security, as it would be confined to specific environments and monitored, rather than in the hands of end users.[237] CTA proposes that, rather than a blanket prohibition for any importation, marketing, or sale of equipment on the covered list, we instead prohibit authorization for certain uses while preserving marketplace employment of such equipment in circumstances and contexts that do not implicate national security concerns.[238]

91. We recognize that commenters have raised points related to technical concerns and the intended use of imported equipment. However, as with the other rule revisions that we are adopting in this item, we focus review of our importation and marketing rules on how they relate to addressing equipment on the Covered List in terms of equipment authorization. We emphasize that, generally under our rules, RF devices may be imported only when certain conditions are met.[239] Many of those conditions are based on equipment authorization, with other very limited conditions based on personal use, demonstration, and other very restrictive conditions. As such, we find that, at this time, there is no need to adopt revisions to our importation or marketing rules to address equipment on the Covered List because our revisions to the equipment authorization rules prohibiting any further authorization of covered equipment also serve to prohibit the importation and marketing of such equipment.

5. Exempt equipment

92. As a general matter, the Commission's equipment authorization program is concerned with ensuring that RF emissions do not cause harmful interference to radio communications. However, in the *NPRM*, the Commission recognized that this proceeding involves concerns about equipment that poses an unacceptable risk to our nation's communications networks, which are distinct from the Commission's concerns related to interference to authorized radio services. Asking whether "covered" equipment potentially could include equipment that currently is exempt from its equipment authorization processes, the Commission sought comment on whether to reconsider whether, in order to address security concerns, providing such exemptions continues to be appropriate.

93. *Background.* The most diverse set of exempt devices operate under our part 15 unlicensed device rules. Certain unlicensed RF devices are exempt from demonstrating compliance under either of our equipment authorization procedures (certification or SDoC) because these devices generate such low levels of RF emission that they have little potential for causing harmful interference to authorized radio services, although some devices may be exempt for other reasons [240] In addition, certain equipment that operates within licensed services are also exempt from part 2 equipment authorization due

[234] Huawei Cos. Comments at 19.

[235] Dahua USA Comments at 21.

[236] CTA Comments at 22.

[237] *Id.* at 22-23.

[238] *Id.* at 16.

[239] *See* 47 CFR § 2.1204(a) ("Import conditions").

[240] 47 CFR § 15.103. Under this rule part certain digital devices are exempt from equipment authorization procedures.

to a variety of reasons beyond interference concerns[241] and are not subject to the Commission's specific part 2 testing, filing, or record retention requirements. However, such devices are subject to complying with the unique operational and technical requirements associated with the particular licensed service.

94. In the *NPRM*, the Commission sought specific comment on whether the Commission should revise its rules to eliminate any equipment authorization exemption for "covered" equipment based on the potential of such equipment, regardless of RF emissions characteristics, to pose an unacceptable risk to U.S. networks or users. The Commission further sought comment on whether such a revision should apply only to exempt part 15 unlicensed devices or should include currently exempt devices that operate under other rule parts. The Commission also asked whether to require that any equipment (in whole or in part), regardless of any applicable rule exemption, that is produced by any entity that has produced "covered" equipment on the Covered List be processed pursuant to the Commission's certification process (similar to the proposal and the requirement that we are adopting that such entities must use the certification process for equipment, even if existing rules had permitted processing through the SDoC process).

95. Some commenters oppose removing the existing exemption, indicating either full or partial support for retaining an equipment authorization exemption, even if the equipment is determined to be "covered." For instance, ITI recommends that the Commission avoid seeing a national security threat in every unintentional radiator; ITI maintains that the exempt class of devices and unintentional radiators exists precisely because of the low interference potential. In addition, ITI argues that the FCC should not proceed with unilaterally expanding its authority over part 15 and other exempt devices and components beyond existing statutory authority related to RF interference complaints. Similarly, CTA argues that changing the exempt status of some equipment would overstep the Commission's charter for RF emissions and safety and could create a logjam in the equipment authorization process.[242] i-Pro requests that the Commission not revise its current regulations to require that any exempt devices produced by an entity that has produced equipment included on the Covered List be subject to the Commission's certification rules and processes.[243] Brunner, however, supports Commission action to no longer exempt any "covered" devices that pose a low risk of harmful interference if such devices pose an unacceptable risk to the national security of the United States. This commenter recommends that the Commission revise any relevant rules to no longer provide authorization exemptions to such equipment, and not limit this revision to devices subject to any particular rule part.[244]

96. In the *NPRM*, the Commission tentatively concluded that the legal authority associated with the Commission's proposal to prohibit authorization of "covered" equipment in its equipment authorization process also provided, pursuant to section 302 and section 4(i) of the Act, for actions that the Commission might take with respect to precluding "covered" equipment from being exempted from the equipment authorization process.

97. *Discussion.* We conclude that the Commission will no longer exempt "covered" communications equipment, i.e., equipment that has been determined to pose an unacceptable risk to national security pursuant to the Secure Networks Act from equipment authorization requirements. Accordingly, we will require that any equipment produced by any of the entities identified on the Covered List as producing "covered" equipment to be processed through the certification process just as we are requiring equipment previously subject to the SDoC procedures to be processed through the certification processes. By no longer exempting equipment produced by these entities, the Commission is taking

[241] Examples include, but are not limited to, most earth stations and space stations under part 25, transmitting equipment used in the band 1427-1435 MHz under part 90 (47 CFR § 90.203(b)(3)), and equipment used in the Amateur Radio Service under part 97 (except for external RF power amplifiers).

[242] CTA Comments at 20-21.

[243] i-Pro Comments at 1-2.

[244] Brunner Comments at 23-25.

another step to protect our nation's supply chain from new equipment that has been determined to be "covered."

98. As noted in the *NPRM*, certain RF equipment that for various reasons has been exempted from the need to demonstrate compliance under the Commission's equipment authorization procedures, which are generally concerned with ensuring that devices do not cause harmful interference to authorized radio services. Also as discussed in the *NPRM*, this proceeding involves concerns about equipment that poses an unacceptable risk to our nation's communications networks, which are distinct from the Commission's concerns related to harmful interference to authorized radio services. Whether communications equipment poses an unacceptable risk to national security simply does not turn on considerations of RF interference. Nor is the Secure Networks Act or Secure Equipment Act so concerned.

99. We conclude that certain types of equipment that is currently exempt from equipment authorization requirement and produced by entities identified on the Covered List could constitute "covered" equipment. Later in this Report and Order we discuss certain types of communications equipment that is "covered" equipment. Among other things, we conclude that, for purposes of implementing our prohibition on "covered" equipment, such equipment includes "access layer," "distribution layer," and "core layer" equipment produced by entities identified on the Covered List and that is used in networks providing advanced communications services.[245] Pursuant to section 5 of the Secure Networks Act, the Commission requires that advanced communications service providers report whether they have purchased, leased, rented, or otherwise obtained such "covered" equipment (after August 18, 2018).[246] "Access layer" equipment is equipment associated with providing and controlling end-user access to the network over the "last mile," "local loop," or "to the home" (e.g., optical terminal line equipment, optical distribution network devices, customer premises equipment (to the extent owned by the advanced services provider), coaxial media converters, wavelength-division multiplexing (WDM) and optical transporting networking (OTN) equipment, and wireless local area network (WLAN) equipment). "Distribution equipment" includes middle mile, backhaul, and radio area network (RAN) equipment (e.g., routers, switches, network security equipment, WDN and OTN equipment, and small cells). "Core layer" equipment is associated with the backbone infrastructure (e.g., optical networking equipment, WDN and OTN, microwave equipment, antennas, RAN core, Cloud core, fiber, and data transmission equipment).[247] Thus, to the extent that equipment currently exempt from equipment authorization procedures is produced by any entity identified on the Covered List, such equipment will no longer be eligible for such exemption and must seek authorization through the certification process, and we will revise our part 15 rules to so indicate.

100. Similar to our decision to no longer permit these entities to avail themselves of the SDoC process, requiring all equipment they produce to undergo more rigorous scrutiny as well as complying with the attestation requirements is the best way the Commission can fulfil its statutory obligation to ensure that "covered" equipment is no longer able to be purchased and used thereby protecting national

---

[245] *See infra,* section III.C.5.

[246] *See Supply Chain 2nd R&O*, 35 FCC Rcd at 14369, para. 212; 47 CFR § 1.50007.

[247] *See Supply Chain Annual Reporting 2022 Filing Instructions* at 25; "Protecting the Communications Supply Chain, Information Collection, Network Categories," https://us-fcc.app.box.com/v/NetworkCategories

We also note that the Commission had directed the Wireline Competition Bureau (WCB), in implementing the Secure Networks Act Reimbursement Program to develop a "Catalog of Expenses Eligible for Reimbursement." *Supply Chain 2nd R&O*, 35 FCC at 14339-40, paras. 128-29; *see* 47 CFR § 1.50004(p). The catalog ultimately developed by WCB and published on the Commission's website similarly identified categories of equipment – including Huawei and ZTE equipment in the "access layer," the "distribution layer," and the "core layer" of a communications network – that would be eligible for purposes of reimbursement under the Reimbursement Program. *See Final Catalog of Eligible Expenses and Estimated Costs* (Revised December 17, 2021), found at https://www.fcc.gov/sites/default/files/scrp-final-catelog-eligible-expenses-estimated-costs-12172021.pdf.

security. We further conclude that the measures that we are taking are consistent with our long-standing legal authority (as discussed above) and are reasonable and appropriate both to prohibit authorization of "covered" equipment on the Covered List pursuant to the Secure Networks Act and to further comply with Congress's mandate in the Secure Equipment Act.

6. Revocation of authorizations of "covered" equipment

101. In the *NPRM*, the Commission sought comment on revocation of equipment authorizations on the grounds that the equipment authorization involved "covered" equipment. The Commission tentatively concluded that, if it adopted new rules prohibiting authorization of "covered" equipment, the Commission had the authority to revoke any authorization that may have been granted after adoption of such rules based on applicants' false statements or representations that the equipment was not "covered."[248] The Commission also tentatively concluded that the current rules provide the Commission with the authority to revoke any *existing* equipment authorizations – i.e., authorizations granted before adoption of rules in this proceeding prohibiting any future authorization of "covered" equipment – if such equipment constituted "covered" equipment,[249] and sought comment on whether there are particular circumstances that would merit revocation of any specific equipment authorization(s) and if so, the procedures that should apply (including whether to adopt possible revisions to the current procedures).[250]

102. With respect to equipment authorized subsequent to adoption of proposed rules prohibiting authorization of "covered" equipment, the Commission tentatively concluded that section 2.939(a)(1)-(2) applied to "covered" equipment, such that the Commission could revoke any equipment authorization that may have been granted based on false statements or representations in the application for authorization attesting that the equipment is not "covered." Under this proposed approach, the Commission would revoke any such equipment authorization granted after adoption of the rules proposed in the *NPRM*, even if the TCBs or the Commission had not acted to set the grant aside within the 30-day period following the posting of the grant on the EAS database.[251] In addition, the Commission tentatively concluded that, pursuant to section 2.239(a)(3),if authorized equipment is subsequently changed (e.g., the responsible party initiates a permissive change which changes the equipment status from not covered to "covered" equipment), that equipment authorization could be revoked because such a change, would violate the Commission's newly adopted prohibition on authorization of "covered" equipment.[252]

103. As for revocation of any existing equipment authorizations involving "covered" equipment, the Commission sought comment on whether section 2.939(a)(4), which allows revocation '[b]ecause of conditions coming to the attention of the Commission which would warrant it in refusing to grant an original application" would provide the Commission basis for revoking equipment granted prior to adoption of the prohibition on authorization of "covered" equipment.[253] In addition, the Commission tentatively concluded, if it were to adopt rules prohibiting authorization of "covered" equipment, then section 2.939(c), which states that the Commission "may also withdraw any equipment authorization in the event of changes in its technical standards," could constitute such a change in technical standards that warrants withdrawal of the equipment authorizations.[254]

104. To the extent the Commission sought to revoke any equipment authorizations, it noted the current procedures set forth in section 2.939(b), and requested comment on whether it should use

[248] *NPRM*, 36 FCC Rcd at 10611-12, para. 82.

[249] *Id.* at 10611-12, paras. 83-84.

[250] *Id.* at 10611-13, paras. 83-89.

[251] *Id.* at 10611-12, para. 83.

[252] *Id.* at 10612, para. 84.

[253] *Id.* at 10612, para. 85.

[254] *Id.* at 10612, para. 86.

these specific procedures or other procedures, and on what process the Commission could use to help identify equipment authorizations for revocation.[255] Finally, the Commission asked whether it should make any revisions to section 2.939, including whether that section should specifically address the revocation process for "covered" equipment.[256]

105. No commenting party disputes that the Commission has the authority to revoke equipment authorizations in instances when applicants provide false statements or representations, the equipment does not conform to technical requirements, or unauthorized changes are made to equipment. For example, the Information Technology Industry Council (ITI) and Huawei Cos. state in their respective comments that revocation of equipment authorization is reasonable under those circumstances.[257] Huawei Cos. contend, however, that none of these provisions would provide grounds for revoking existing authorizations.[258] As for the applicability of particular provisions, ITI contends that section 2.939(c)(4) does not provide the Commission a basis for revoking existing authorizations, maintaining that any conditions that may come to light after certification must have a bearing on the RF emissions analysis or relate to case-specific facts that would have been disqualifying for a particular applicant in the first instance; it argues that permitting revocation under this provision would, in effect, grant the Commission virtually unlimited authority to rewrite the rules of the process arbitrarily and at any time, without regard for whether the new conditions are at all related to the functionality of equipment or its potential to cause RF interference.[259] IPVM, however, asserts that section 2.939(a)(4) allows the Commission to revoke authorizations because of conditions coming to the Commission's attention, particularly with regard to applications filed subsequent to PSHSB's publication of the Covered List in March 12, 2021.[260] IPVM concludes that it would be reasonable to revoke these authorizations for not being in compliance with our overarching mission and mandate, even if the applications were properly prepared under the explicit rules of the equipment authorization program at the time of filing.[261] With regard to the applicability of section 2.939(c), Huawei Cos. and ITI assert that that this does not warrant revocation because a prohibition on "covered" equipment does not involve a change in "technical standards."[262] Most commenters oppose action by the Commission to revoke existing authorizations of "covered" equipment, expressing various concerns about the appropriateness of such revocations, including the potential for adverse impact to consumers and the supply chain.[263]

---

[255] *Id.* at 10612-13, paras. 87-88.

[256] *Id.* at 10613, para. 89.

[257] ITI Comments at 5-6; Huawei Cos. Comments at 8-9.

[258] Huawei Cos. Comments at 8-9.

[259] ITI Comments at 6.

[260] IPVM Jan. 11, 2022 *Ex Parte* at 4-5.

[261] *Id.*

[262] Huawei Cos. Comment at 9; ITI Comments at 5-7.

[263] *See, e.g.*, 5G Americas Comments at 2 (does not support retroactive rescission); CTA Comments at 14 (revocation of existing authorizations could be disastrous for consumers); CTIA Comments at 9-12 (could present serious challenges potentially harming American consumers, and could weaken supply chains by impacting mutual recognition agreements); ITI Council Comments at 5-8 (revocation of "covered" equipment would unmoor the revocation process, present a myriad of practical challenges as well as industry and consumer confusion); NCTA Comments at 9-10 (would create an unfunded "rip" and "replace" mandate); NTCA Comments at 7 (would be highly detrimental to providers that relied on the Commission's rules); TIA Comments at 12 (only proceed if a mechanism exists to reimburse those affected); China Tech Threat Reply Comments at 3, 9-10 (Commission regulation should focus on future prohibitions, not revocation of past authorizations; this would allow the Commission time to communicate to the public on a going-forward basis); *but see* JVC Kenwood Comments at 2, 5-8 (Commission should revoke existing authorizations).

106. The Secure Equipment Act, enacted subsequent to the close of the comment period on the *NPRM*, includes specific provisions concerning the Commission's actions that concern revocation of equipment authorizations involving "covered" equipment. In section 2(a)(2), Congress directed the Commission to adopt new rules prohibiting authorization of "covered" equipment.[264] As for revocation of existing equipment authorizations involving "covered" equipment, section 2(a)(3)(A) of the Act provides that "[i]n the rules adopted" by the statutory deadline, the Commission "may not provide for review or revocation of any equipment authorization" granted before the adoption date of such rules.[265] Section 2(a)(3)(B), however, provides that, other than in "the rules adopted" by the statutory deadline, "[n]othing in this [Act] may be construed to prohibit the Commission … from – (i) examining the necessity of review or revocation of any equipment authorization on the basis of the equipment being on the [Covered List]; or (ii) adopting rules providing for any such review or revocation.[266]

107. In this Report and Order we do not adopt any rules providing for the review or revocation of any currently existing equipment authorization granted prior to adoption of this order. With respect to equipment authorized after adoption in this Report and Order of rules prohibiting authorization of "covered" equipment, we adopt streamlined revocation procedures to apply if the authorization had been granted based on false statements or representations in the applications that the equipment is not "covered," or if the authorized equipment is modified or changed in such a way as to become "covered" equipment. In addition, we conclude that the Commission has the authority, as affirmed by Congress in the Secure Equipment Act, to consider the necessity to review or revoke an existing authorization of "covered" equipment approved prior to adoption of this Report and Order, and that it has such authority to consider such action without considering additional rules providing for any such review or revocation of existing authorizations.

a. Streamlined revocation of authorizations based on false statements or representations about "covered" equipment

108. With regard to revocation of equipment authorizations granted after adoption of rules in this Report and Order prohibiting authorization of "covered" equipment, we conclude, as in the *NPRM*, that the Commission already has authority, under its current rules in section 2.939(a)(1), to revoke authorizations if the Commission discovers, post-authorization, that the application (or in materials or responses submitted in connection therewith) contained false statements or representations.[267] We note that revoking authorizations on this basis is clearly permitted under the Secure Equipment Act, which did not proscribe adopting rules for revocation of authorizations that are granted after adoption of this Report and Order.

109. However, because Congress established that "covered" equipment poses an unacceptable risk to national security, we find that it is necessary to adopt an expedited mechanism for review and revocation of equipment authorizations that were granted after adoption of our prohibitions where the application for such authorization contained a false statement or representation regarding the "covered" status of such equipment at the time of such statement or representation. To that end, we adopt a new provision, section 2.939(d), providing for streamlined procedures , to address such situations, as discussed further below.[268]

---

[264] Secure Equipment Act § 2(a)(2).

[265] *Id.* § 2(a)(3)(A).

[266] *Id.* § 2(a)(3)(B).

[267] 47 CFR § 2.939(a)(1).

[268] The rules we adopt here do not otherwise affect the general applicability of the revocation procedures set forth under section 2.939(b) for existing equipment authorizations. We note, however, that in the Further Notice of Proposed Rulemaking we are seeking comment on possible revisions to the revocation procedures under section 2.939(b) for existing authorizations.

110. Nothing in our statutory authority requires that the process for revocation of equipment authorizations be conducted pursuant to existing rule section 2.939(b), i.e., the revocation process generally afforded radio licensees.[269] As the Commission noted in its 2020 order adopting streamlined procedures for certain administrative hearings, the hearing provisions in the Communications Act do not expressly require formal hearings (e.g., hearings conducted with live witness testimony and cross examination and the introduction of evidence before a presiding officer).[270] Instead, revocation proceedings generally are subject only to informal adjudication requirements under the Administrative Procedure Act, which requires that an authorization holder be given written notice of the facts or conduct which may warrant the revocation and an opportunity to demonstrate or achieve compliance with all lawful requirements.[271] The Commission may resolve disputes of fact in an informal hearing proceeding on a written record. Thus, we conclude that, going forward, where the Commission has reason to believe that an equipment authorization was granted on the basis of a false statement or representation by the applicant concerning whether the subject equipment is "covered" equipment, the more streamlined informal hearing procedures described below, based on a written record, will apply. However, the Commission may in its discretion determine to hold oral hearings when needed to resolve a genuine dispute as to an outcome-determinative fact, and such hearings may be limited to testimony and cross-examination necessary to resolve that dispute.[272]

111. As discussed in the Report and Order above, we also are prohibiting the modification of equipment if such modification would alter the equipment's status such that it would become "covered" equipment.[273] In implementing this prohibition, we require that applications or requests to modify already certified equipment include a written and signed certification that the equipment is not "covered." We conclude that, pursuant to existing section 2.939(a)(3), the Commission already has authority to revoke an equipment authorization granted after our adoption of rules here if that equipment is changed in the future in such a way as to become "covered" equipment. Again, because "covered" equipment poses an unacceptable risk to national security, we also will include within the streamlined procedures the authority to revoke equipment authorization in which equipment is changed in such a way that it becomes "covered" equipment where the application or request for modification is found to include false statements or representations that the equipment is not "covered."[274]

112. *Streamlined procedures*. In cases in which OET and PSHSB, working with other Bureaus/Offices as may be appropriate, have reason to believe that a particular equipment authorization or modification of an equipment authorization granted after adoption of the rules in this Report and Order was or may have been based on a false statement or representation made by applicant, either in the

[269] 47 CFR § 2.939(c).

[270] *See Procedural Streamlining of Administrative Hearings*, EB Docket No. 19-214, Report and Order, 35 FCC Rcd 10729 (2020). We note that there is an exception, which is not relevant here. Specifically, the exception is section 503 of the Act, which authorizes the Commission to impose a forfeiture penalty on a person after "a hearing before the Commission or an administrative law judge thereof in accordance with section 554 of" the APA. 47 U.S.C. § 503(b)(3)(A); *see also* 47 U.S.C. §§ 503(b)(4)(A), 504(a).

[271] 5 U.S.C. § 558(c); *Procedural Streamlining of Administrative Hearings*, EB Docket No. 19-214, Report and Order, 35 FCC Rcd at 10732, para. 10. As the Commission noted, for many types of cases, conducting trial-type hearings imposes unnecessary costs, burdens, and delays. *Id.* at 10731, para 7.

[272] *Cf.* 47 CFR § 1.376. Congress accorded the Commission broad discretion to "conduct its proceedings in such manner as will best conduce to the proper dispatch of business and to the ends of justice." 47 U.S.C. § 154(j); *FCC v. Schreiber,* 381 U.S. 279 (1965).

[273] Section III.B.2(c).

[274] *See NPRM*, 36 FCC Rcd at 10612, para. 84.

application or in the materials connected therewith,[275] regarding the required attestations under revised section 2.911 concerning whether the equipment was "covered" or whether the applicant is an entity identified on the Covered List, OET and PSHSB will investigate whether such authorization was improperly granted or otherwise should be revoked. OET and PSHSB will provide written notice to the equipment authorization holder of the initiation of a revocation proceeding and the grounds under consideration for such revocation. As discussed above, we are requiring that applicants for equipment authorization make certain attestations under section 2.911 regarding the subject equipment in the context of "covered" equipment. False statements or representations with respect to the application under this section provide grounds for revocation of the authorization pursuant to section 2.939(a)(1).

113. We will model this procedure along lines consistent with section 558 of the Administrative Procedure Act.[276] OET and PSHSB will issue an order to show cause why revocation proceedings should not be initiated, which order will provide notice of the facts or conduct which may warrant revocation, and an opportunity to demonstrate or achieve compliance. The equipment authorization holder will have 10 days thereafter to provide a written submission responding to the notice of proposed revocation. After reviewing the record and any supplemental information requested by OET and PSHSB, if they find that the equipment is "covered" or that the applicant did not disclose that it was an entity identified on the Covered List, they will initiate revocation proceedings, providing the basis for such decision. We note that the determination as to whether to revoke an authorization focuses on whether the attestation was true, and it does not require any finding that the applicant has the specific intent to make a false statement or representation. In the event of revocation of an equipment authorization, OET and PSHSB will issue an order explaining its reasons as well as how such revocation will be implemented (e.g., halting distribution, marketing, and sales of such equipment, requiring other appropriate actions) and enforced.

b. Revocation of existing equipment authorizations on grounds that the equipment is "covered" equipment

114. We also conclude that the Commission has the requisite authority under the Communications Act to review any existing equipment authorization that would, under the rules that we adopt in this Report and Order, be "covered" equipment, and to determine the necessity for revoking such authorization, and that the Commission can undertake such revocation pursuant to current rules. We reach this determination based on our reading of the Commission's existing authorities. Pursuant to the same authorities discussed above with respect to the equipment authorization program, the Commission has long relied on its authority (modelled along the lines of section 312 with respect to spectrum licensees[277]) to revoke equipment authorizations under section 2.939(a)(4) "[b]ecause of conditions coming to the attention of the Commission which would warrant it in refusing to grant an original application."[278] We conclude that it is well within the Commission's responsibilities and mandate, as IPVM has suggested,[279] to revoke an existing equipment authorization under section 2.939(a)(4).

115. That the Commission has such authority to revoke is confirmed by the Secure Equipment Act. Indeed, as a matter of statutory structure, the Secure Equipment Act can be read as saying two

[275] Under the rules adopted in this Report and Order, the Commission is prohibiting authorization of "covered" equipment under section 2.903 and various associated part 2 rules. As set forth in sections 2.911(d) and 2.1033, the applicant for an equipment authorization must attest, by written and signed certification, that the equipment is not "covered" equipment. Similarly, under the rules adopted, as set forth in sections 2.932 and 2.1043, when the applicant requests modification of an existing authorization or changes in the equipment certification, it must attest, by written and signed certification, that the equipment is not "covered" equipment.

[276] 5 U.S.C. § 558.

[277] *Id.* § 312(a)(2).

[278] 47 C.F.R. § 2.939(a)(4).

[279] IPVM Jan. 11, 2022 *Ex Parte* at 4-5

complementary things: one, that the Commission has no discretion with respect to reviewing or approving requests for equipment authorization for equipment listed on the Covered List (as discussed above) after the effective date of our Report and Order here -- i.e., the Secure Equipment Act requires that the Commission no longer review or approve them; and, two, that the Commission does have discretion ("other than in the rules adopted" here) to exercise its statutory authority to decide whether to take equipment authorization action regarding authorizations granted prior to the effective date of our decision here.

116. First, in sections 2(a)(1) and 2(a)(2), Congress determined that the Commission shall adopt rules that clarify – on a going forward basis – that the Commission will no longer review or approve equipment that is on the Covered List. This is reinforced by Congress's inclusion of section 2(a)(3)(A), which specifically states that "[i]n the rules adopted under paragraph [2(a)](1)," i.e., the rules we adopt today in this Report and Order, "the Commission may not provide for review or revocation of any equipment authorization granted before the date on which such rules are adopted on the basis of the equipment being on the [Covered List]." Read together, sections 2(a)(1), 2(a)(2), and 2(a)(3)(A) state that, with respect to the scope of the Commission's section 2(a)(2) rules, those rules shall not provide for the review or revocation of existing authorizations. Second, in section 2(a)(3)(B), Congress made clear that the Commission could use its existing authority to adopt non-section 2(a)(2) rules or otherwise examine the necessity of providing for the review or revocation of equipment authorizations granted before the effective date of any section 2(a)(2) rules – even in cases where the sole basis for the Commission's equipment authorization action in those circumstances is the equipment being included on the Covered List.

117. Thus, with regard to the Commission's discretion under the Secure Equipment Act, with regard to new equipment authorizations going forward, Congress has taken the discretion out of the Commission's hands and directed us to stop reviewing or approving applications involving "covered" equipment. Congress has exercised its authority to draw a bright and clear line. As for existing equipment authorizations, Congress has preserved the Commission's existing authority – and the discretion that comes with the exercise of that authority – to decide whether we should take action based on equipment being added to the Covered List.

118. Finally, we note that we are making no decision in this Report and Order as to whether any particular existing equipment authorization should be revoked. Whether and to what extent and pursuant to what processes the Commission exercises that authority would be based on several considerations, including the public interest and our assessment of the costs and benefits of any such action. As noted above, the procedures for revoking authorizations that would be applicable to authorization(s) granted before adoption of these rules are set forth in section 2.939(b). In our Further Notice of Proposed Rulemaking below, we explore streamlining these procedures and seek comment on other issues relating to revocation.

C. "Covered" Equipment

119. As discussed above, in the *NPRM* the Commission proposed revisions to its equipment authorization rules and procedures under part 2 to prohibit authorization of any "covered" equipment that is identified on the Covered List published by PSHSB.[280] As noted, this Covered List identifies certain equipment that, to date, has been determined – pursuant to the Secure Networks Act – to be communications equipment that poses an unacceptable risk to national security and safety of U.S. persons.[281] Equipment is on the Covered List only if one of four enumerated sources determines such

[280] *NPRM*, 36 FCC Rcd at 10596, 10600, paras. 38, 40, 47. As discussed above, the Commission also sought comment on whether any "covered" equipment that is currently exempted from the need for authorization no longer be exempted, and whether it should revoke any existing authorizations. *See NPRM*, 36 FCC Rcd at 10610, 10611-13, paras. 76-79, 83-89. This proceeding is focused on "covered" equipment, and does not address issues related to "covered" services that are also included on the Covered List.

[281] Secure Networks Act § 2(a)-(c).

equipment "poses an unacceptable risk to the national security of the United States or the security and safety of United States persons."[282] As future determinations are made by these four enumerated sources about "covered" equipment are made, PSHSB will update the Covered List to reflect those determinations..[283]

120. In the *NPRM*, the Commission proposed and sought comment on how to identify and address particular "covered" equipment that would no longer be permitted to obtain equipment authorizations. Comments on the scope of what constitutes "covered" equipment vary widely (as discussed in detail below). Several commenters ask for Commission clarification of what constitutes "covered" equipment for the purposes of the instant proceeding.[284] We agree that sufficient clarity is needed to provide guidance for purposes of administering the prohibition on authorization of "covered" equipment in the Commission's equipment authorization program pursuant to our part 2 rules. As discussed in the *NPRM*, the Commission's efforts to revise its equipment authorization program rules to prohibit authorization of "covered" equipment is one of several different efforts by the Commission as well as various Federal agencies, including those pursuant to the Secure Networks Act and section 889 of the 2019 NDAA, to identify and prohibit the use of "covered" equipment that poses an unacceptable risk to national security.[285] Several commenters, including industry associations express concern that the Commission not take actions in the instant proceeding that would create confusion or conflict with other Commission actions (e.g., the Commission's Reimbursement Program), and otherwise stress the importance that the Commission work with other Federal agencies on these concerns.[286]

121. Below, we discuss what constitutes "covered" equipment for purposes of the Secure Networks Act, as implemented by the Commission and placed on the Covered List, and the Secure Equipment Act. This includes discussion of the equipment that already has been included on the Covered List to date, specifically "telecommunications equipment" and "video surveillance equipment" produced by five named entities – Huawei, ZTE, Hytera, Hikvision and Dahua – pursuant to the Secure Networks Act and the determination made by Congress in section 889(f)(3) of the 2019 NDAA. For purposes of implementing the prohibition of the authorization of such equipment in our equipment authorization process, we provide guidance on the scope of "covered" equipment. Because the equipment placed on the Covered List is expected to evolve over time based on new determinations concerning equipment made outside of the Commission, we also discuss how any future such determinations will be addressed with respect to prohibiting authorizations of "covered" equipment in the Commission's equipment authorization program.

1. Statutory background

122. As discussed above, the rules we adopt in this Report and Order are based on various sources of statutory authority and our instructions from Congress, including in the Communications Act of 1934, as amended, the Secure Networks Act, and the Secure Equipment Act of 2021, to use such authorities to protect the public interest, including the national security of the United States and the safety

[282] 47 U.S.C. § 1601(b)(1), (c); 47 CFR § 1.50002(b)(1).

[283] As noted above, the Covered List was recently updated.

[284] *See, e.g.*, Hytera US Comments at 5-6; NTCA Comments at 4-5; i-Pro Comments at 2; Motorola Mar. 24, 2022 *Ex Parte* at 5-6.

[285] *NPRM*, 36 FCC Rcd at 10580-89, paras. 6-22.

[286] CTIA Comments at 11-12 (approach regarding prohibiting equipment authorization in this proceeding should not cause substantial uncertainty or confusion vis a vis the Commission's actions concerning its "rip and replace" program involving equipment on the Covered List); NTCA Comments at 3 (the Commission's proposal would also duplicate efforts already undertaken by other federal agencies, including NIST and NTIA, to prompt equipment manufacturers to build more security into their products); Johnson/Tatel Comments at 1 (Commission actions should be undertaken with close coordination with industry and interagency partners to avoid unintended practical and legal consequences).

and security of United States persons.[287] This background provides the bases for our considerations in this proceeding of what constitutes "covered" communications equipment for the purposes of the rules that we adopt today and the actions that this Commission is taking in the instant proceeding with regard to prohibiting future authorization of such equipment

123. *The Secure Networks Act.* Pursuant to the Secure Networks Act, the equipment on the Commission's Covered List is based exclusively on determinations made by any one of four specified, enumerated sources in the Federal government that are outside of the Commission.[288] In addition, the Secure Networks Act contemplates that what constitutes "covered" equipment on the Covered List will evolve over time as the determinations from the enumerated sources evolve.[289]

124. Section 2(a) of the Secure Networks Act provides that "the Commission shall publish on its website a list of covered communications equipment or services."[290] Section 2(b) directs the Commission to publish a list of covered communications equipment or services if, and only if, one or more determinations is made by four enumerated sources, and the equipment or service "is capable of" (A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles, (B) causing the network of a provider of advanced communications service to be disrupted remotely; or (C) otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons.[291]

125. Section 3(c) of the Secure Networks Act specifically directs the Commission to place on the Covered List any communications equipment or service "based solely on one or more of the following determinations":

(1) A specific determination made by any executive branch interagency body with appropriate national security expertise, including the Federal Acquisition Security Council established under section 1322(a) of title 41, United States Code.
(2) A specific determination made by the Department of Commerce pursuant to Executive Order No. 13873 (84 Fed. Reg. 22689; relating to securing the information and communications technology and services supply chain).
(3) The communications equipment or service being covered telecommunications equipment or services, as defined in section 889(f)(3) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232; 132 Stat. 1918).
(4) A specific determination made by an appropriate national security agency.[292]

Section 9 of the Secure Networks Act defines "communications equipment" as "any equipment … that is essential to the provision of advanced communications service," which it defines as "ha[ving] the meaning given the term 'advanced communications capability' in section 706 of the Telecommunications Act of 1996."[293]

126. *Commission interpretations of the Secure Networks Act; part 1 rules.* In its 2020 *Supply Chain 2nd R&O*, the Commission began its efforts to implement the Secure Networks Act. In so doing, the Commission examined the Secure Networks Act's applicability to "communications equipment or

[287] *See supra* Section **Error! Reference source not found.**; 47 U.S.C. §§ 151, 1601; Secure Equipment Act.

[288] Secure Networks Act, §§ 2(b)(1).

[289] *Id.* § 2(d).

[290] *Id.* § 2(a).

[291] *Id.* § 2(b).

[292] *Id.* § 2(b)-(c).

[293] *Id.* § 9(4) and 9(1), respectively.

service" and to providers of "advanced communications service" and how those terms should be construed for the purposes of implementing rules, which have been incorporated in its part 1 rules.[294]

127. Specifically, the Commission interpreted what would be deemed "communications equipment and services" that are, per the Secure Networks Act, "essential to the provision of advanced communications service." It concluded that this includes "all equipment and services used in fixed and mobile broadband networks, provided they include electronic components."[295] Accordingly, section 1.50001(c) of the Commission's rules provide as follows:

> *Communications equipment or service.* The term "communications equipment or service means any equipment or service used in fixed and mobile networks that provides advanced communications service, provided the equipment or service includes or uses electronic components.[296]

The Commission concluded that all equipment or services that include or use electronic components can "reasonably be considered essential to broadband networks" as it sought to provide a "bright line rule" that would "ease regulatory compliance and administrability" and also would provide "regulatory certainty" for compliance purposes.[297]

128. Next, the Commission interpreted "advanced communications service" for purposes of the Secure Networks Act to include services with any connection of at least 200 kbps in either direction, which is consistent with the Commission's historic interpretation of section 706 of the Telecommunications Act.[298] In adopting this definition, the Commission recognized that it was taking a broad, more inclusive approach to the scope of equipment and services that is deemed "covered," which it viewed consistent with Congressional intent. In particular, the Commission noted that, while it had been encouraging advanced communications service providers to offer broadband service at greater speeds, it interpreted "advanced communications service" in this proceeding to include the slower 200 kbps threshold, concluding that "cover[ing] a broader array of equipment and services," including older legacy technology, the Commission's approach would to be "consistent with congressional intent to identify and remove insecure equipment."[299] Accordingly, the Commission adopted the following definition in section 1.50001(a):

> *Advanced communications service.* The term "advanced communications service" means high-speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology with connection speeds of at least 200 kbps in either direction.[300]

129. *"Covered" communications equipment and the Commission's Covered List.* As set forth in section 2(a) of the Secure Networks Act, the Commission is required to publish a list of "covered" communications equipment or services.[301] The Commission's part 1 rules provide that PSHSB must publish the Covered List and place on that list any such equipment produced by any entity if, based exclusively on any of those determinations, such equipment poses an unacceptable risk to the national security of the United States or the security and safety of United States persons and meets certain

---

[294] *See Supply Chain 2nd R&O*, 35 FCC Rcd 14284.

[295] *Id.* at 14308, para. 52.

[296] 47 CFR § 1.50001 Definitions, § 1.50001(c)

[297] *Supply Chain 2nd R&O*, 35 FCC Rcd at 14308, para. 52.

[298] *Id.* at 14310-11, para. 55.

[299] *Id.* at 14310-11, para. 55.

[300] 47 CFR § 1.50001 Definitions, §§ 1.50001(a).

[301] Secure Networks Act § 2(a).

specified capability requirements.[302] As noted above, PSHSB also must maintain and update that list based on any subsequent updates concerning those determinations.[303]

130. *"Covered" equipment based on determinations to date – Section 889(f)(3) of the 2019 NDAA.* As discussed in the Secure Networks Act, what constitutes "covered" equipment is based on determinations by any one of the four enumerated sources set forth in section 2(c). To date, the current "covered" equipment is on the Covered List based on the determination made pursuant to section 2(c)(3) of the Secure Networks Act, namely Congress's determination under section 889(f)(3) of the 2019 NDAA. Specifically, the first iteration of the Covered List, which had been published before passage of the Secure Equipment Act, included only the determination made by Congress concerning certain "telecommunications equipment" and "video surveillance equipment" as provided under section 889(f)(3)of the 2019 NDAA.[304] As discussed more fully below, section 889(f)(3) addresses in particular the national security concern posed by certain equipment by five named entities or their subsidiaries or affiliates. It states that the term "covered telecommunications equipment or services" includes "telecommunications equipment or services produced by Huawei or ZTE (and their subsidiaries and affiliates) and "video surveillance and telecommunications equipment produced by Hytera, Hikvision, and Dahua (and their subsidiaries and affiliates) "[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes."[305] Thus, when the Commission issued the *NPRM* in this proceeding, in which it proposed to prohibit future authorizations of equipment on the Covered List, the only such equipment was that identified under section 889(f)(3), i.e., telecommunications equipment and video surveillance equipment produced by five entities – namely Huawei, ZTE, Hytera, Hikvision, and Dahua – and their respective subsidiaries and affiliates.[306] This remains true as of the date of this Report and Order.[307]

131. *The Secure Equipment Act*. Against the backdrop of the *NPRM* and the initial version of the Covered List, Congress passed the Secure Equipment Act of 2021, which provides that, for purposes of the instant equipment authorization proceeding (ET Docket No. 21-232), in which the Commission has proposed prohibiting future authorizations of "covered" equipment:

> [T]he Commission shall clarify that [it] will no longer review or approve any application for equipment authorization for equipment that is on the list of covered communications equipment or services published by the Commission under section 2(a) of the [Secure Networks Act].[308]

---

[302] 47 CFR § 1.50002(a)-(b). As for the specified capability requirements, the equipment must be capable or any of the following: (A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles; (B) causing the network of a provider of advanced communications service to be disrupted remotely; or (C) otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons. *Id.* § 1.50002(b)(2).

[303] 47 CFR §§ 1.50002(a), 1.50003(a).

[304] 2019 NDAA § 889(f)(3). The NDAA of 2019 was enacted into law on August 13, 2018. While there have been additional determinations, they have involved covered services, not covered equipment.

[305] *Id.*

[306] In the *NPRM*, the Commission specifically identified these entities as being on the then-existing Covered List. *NPRM*, 36 FCC Rcd at 10595-96, para. 37.

[307] We note that, to date, the Covered List does not at this time include any telecommunications equipment or video surveillance equipment identified by the Secretary of Defense pursuant to section 889(f)(3)(D).

[308] Secure Equipment Act.

In the legislative history accompanying the Secure Equipment Act, the House Committee on Energy and Commerce Report stated that the legislation aimed "to ensure that the Federal Communications Commission did not approve radio frequency devices that pose a national security risk."[309]

2. Current "covered" equipment on the Covered List

132. As discussed above, in the *NPRM* the Commission proposed revisions to its equipment authorization rules and procedures under part 2 to prohibit authorization of any "covered" equipment that is identified on the Covered List published by PSHSB.[310] At the time that the *NPRM* was adopted in June 2021, the only *equipment* on the Covered List, published pursuant to section 2(c) of the Secure Networks Act, was based on the determination under section 2(c)(3) of that Act, namely Congress's determination under section 889(f)(3) of the 2019 NDAA concerning equipment produced by five entities –Huawei, ZTE, Hytera, Hikvision, and Dahua (and their respective affiliates and subsidiaries).[311] We note that, although PSHSB updated the Covered List in March 2022 and in September 2022 to include additional "covered" services and products, the list regarding "covered" equipment has not been updated or otherwise revised.[312] Accordingly, we discuss the "covered" equipment with respect to these same five entities below, the same equipment on the Covered List as discussed in the *NPRM*.

133. As the Secure Networks Act makes clear, "covered" equipment only includes equipment determined by any of the four enumerated sources to pose an unacceptable risk.[313] The Commission has affirmed this in the instant proceeding as it has in earlier decisions by the Commission.[314] Accordingly, we disagree with any assertion by commenters that the Commission should prohibit authorization of any

[309] Report to accompany H.R. 3919, the Secure Equipment Act of 2021, Report 117-148, at 1. As for "Purpose and Summary," the House Report stated that the Act requires the [Commission] to adopt rules to update the equipment authorization procedures to ensure only trusted radio frequency devices are authorized for use in the United States. *Id.* at 2. Finally, as regards "Background and Need for Legislation," the Report states as follows: "While the Secure and Trusted Communications Networks Act took important steps to remove compromised equipment from American networks, the law did not cover equipment that is purchased using private funds (i.e., without the use of federal funds provided by the Commission) and poses a similar national security threat as is conceived under the Act. There is a need to address the national security risks posed by such privately purchased equipment that transmits over radio frequencies, which federal law requires to be licensed by the [Commission]." *Id.* at 2-3.

[310] *NPRM*, 36 FCC Rcd at 10596, 10608, paras. 38, 40, 70. The Commission also sought comment on whether to revoke any existing authorizations of "covered" equipment. *Id.* at 10611-13, paras.80-89. The instant proceeding does not address "covered services."

[311] *Id.* at 10596, para. 37 (citing PSHSB's March 12, 2021 Public Notice on the Covered List).

[312] On March 25, 2022, PSHSB updated the Covered List to include Kaspersky-branded products, based on new determination by the Department of Homeland Security, and China Telecom and China Mobile International USA services, based on determinations made by the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector. On September 20, 2022, PSHSB updated the Covered List to include a determination by the Department of Justice, in coordination with and concurrence of the Department of Defense, to include services offered by PacNet/ComNet and China Unicom. *March 2022 Covered List Public Notice*; *September 2022 Covered List Public Notice.* Both of the updated Covered Lists continued to include on that list the "covered" equipment identified in PSHSB's March 12, 2021 Public Notice on the Covered List. *March 2022 Covered List Public Notice*; *September 2022 Covered List Public Notice.*

[313] Secure Networks Act § 2(c) (the Commission shall place on the Covered List any communications equipment that poses an unacceptable risk based *solely* on one of the four enumerated sources).

[314] *NPRM*, 36 FCC Rcd at 10585-86, para. 15 (citing section 2(c) of the Secure Networks Act and *Supply Chain 2nd R&O*); *Supply Chain 2nd R&O*, 35 FCC Rcd 14311-12, paras. 58-60; *see also id.* at 14324, para. 89.

equipment that has not been determined to pose an unacceptable risk by the four enumerated sources and placed on the Covered List.[315]

134. In the *NPRM*, the Commission proposed that OET, with assistance from Bureaus across the agency (including PSHSB, WCB, WTB, IB, and EB), develop necessary guidance for use by all interested parties – including applicants and TCBs that help administer the equipment authorization program – as the Commission implements the proposed prohibition on future authorizations of "covered" equipment.[316] We first discuss what, in the first instance, is "covered" equipment on the current Covered List for purposes of the prohibition in our equipment authorization program. We then provide further Commission guidance on the types of equipment that will be included with regard to implementing and administering the Commission's prohibition of future authorizations of "covered" equipment under our revised equipment authorization program rules that we are adopting in this Report and Order.[317]

a. "Covered" equipment produced by Huawei and ZTE

(i) Background

135. *The Secure Networks Act and section 889(f)(3) of the 2019 NDAA.* As discussed above, pursuant to the Secure Networks Act 2(c)(3) and section 889(f)(3)(A) and (C) of the 2019 NDAA,[318] PSHSB placed equipment produced by Huawei and ZTE on the initial Covered List published on March 12, 2021, and this equipment is included on subsequent updates to the Covered List.[319] With respect to these two entities, the 2019 NDAA states that "covered telecommunications equipment and services" means:

> (A) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).
> (B) …
> (C) Telecommunications or video surveillance services provided by such entities or using such equipment.[320]

136. *Commission interpretation of "covered" equipment under section 889(f)(3)(A) and (C).* In the *Supply Chain 2nd R&O*, the Commission discussed the section 889(f)(3)(A) and (C) determinations in the 2019 NDAA with respect to Huawei and ZTE equipment.[321] The Commission concluded that, per Congress's section 889(f)(3)(A) determination, it would place on the Covered List "telecommunications equipment produced or provided by Huawei or ZTE" that is capable of the functions outlined in sections 2(b)(2)(A), (B), or (C) of the Secure Networks Act.[322] Furthermore, it rejected Huawei's argument that in order to be "covered" the equipment must be either capable of routing or redirecting user data traffic (per 2(b)(2)(A)) or permitting visibility into any user data or packets (per 2(b)(2(B)), stating instead that "to

---

[315] Two commenters assert that the Covered List should be expanded to include certain equipment by additional entities. Brunner Comments at 3-4, 10-11 (contending that equipment produced by Da Jiang Innovations (DJI), Lenovo, Lexmark, and GoPro should be on the Covered List); China Tech Threat Comments at 24, 33 (equipment by Lenovo and Yangtze Memory Technologies Company should be candidates for the Covered List).

[316] *NPRM*, 36 FCC Rcd at 10600-01, 10606; paras. 49, 63.

[317] *See* Section III.C.5.

[318] *See* Secure Networks Act § 2(c)(3); section 889(f)(3)(A) and (C) of the 2019 NDAA.

[319] *March 2021 Covered List Public Notice* at 2 and n.12 (specifically citing section 889(f)(3) of the 2019 NDAA; Appendix). *See March 2022 Covered List Public Notice*, Appendix; *September 2022 Covered List Public Notice*, Appendix). As discussed below, section 889(f)(3) also identifies equipment produced by Hytera, Hikvision, and Dahua (and their subsidiaries and affiliates).

[320] 2019 NDAA § 889(F)(3)(A), (C).

[321] *Supply Chain 2nd R&O*, 35 FCC Rcd at 14315-16, paras. 66-67, 69.

[322] *Id.* at 14315-16, para. 67.

limit the [§ 889(f)(3)] NDAA determination to equipment capable of routing or permitting network visibility would both ignore the plain text of the NDAA and read section 2(b)(2)(C) out of the Secure Networks Act."[323] The Commission also concluded that Congress' section 889(f)(3)(C) determination required the Commission to include on the Covered List "video surveillance services produced or provided" by Huawei or ZTE or "using such equipment."[324]

137. In the *Supply Chain 3rd R&O*, adopted in July 2021, the Commission further buttressed this conclusion. It noted that, consistent with the Secure Networks Act statutory obligation, the Commission placed on the Covered List the determination found in section 889(f)(3)(A), that is "telecommunications equipment produced or provided by Huawei or ZTE" capable of the functions listed in sections 2(b)(2)(A), (B), or (C). Specifically, it concluded that, per section 889(f)(3), the Commission incorporated *all* such Huawei and ZTE communications equipment into the Covered List.[325] The Commission further concluded that Congress, by including section 2(b)(2)(C) in the Secure Networks Act – i.e., including equipment and services capable of "otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons" – indicated Congress's intent to encompass on the Covered List equipment beyond the narrower list of functions set forth in sections 2(b)(2)(A) or (B) (i.e., capabilities associated with routing or redirecting data traffic or causing the network of a provider of advanced communications service to be disrupted remotely).[326]

138. *The current Covered List.* Regarding Huawei and ZTE, the initial Covered List published in March 2021 stated that the "covered" equipment included: "Telecommunications equipment" produced by these entities (and their subsidiaries and affiliates), "including telecommunications or video surveillance services produced or provided by such [entities] or using such equipment."[327] The subsequent Covered List in March 2022 and the current Covered List published on September 30, 2022 continue to list this same equipment.[328]

139. *Commission prohibitions concerning Huawei and ZTE equipment.* As discussed above, the Commission already has adopted and implemented certain requirements that apply to Huawei and ZTE equipment. For instance, the Commission has established the Reimbursement Program to assist providers of advanced communications service with costs reasonably incurred for the removal, replacement, and disposal Huawei and ZTE communications equipment or services.[329] The Commission also prohibited the use of any Federal subsidy administered by the Commission for support for capital expenditures necessary for the provision of advanced communications services to purchase, rent, lease, otherwise obtain, or maintain any "covered" equipment or services," which the rule defines as communications equipment or service on the Covered List; Huawei and ZTE equipment (as well as

---

[323] *Id.* at 14315-16, para. 67; *see id.* at 14320, para. 80 (if a determination by one of the four enumerated sources indicates that a specific piece of equipment or services poses an unacceptable risk, the Commission will automatically include this determination on the Covered List).

[324] *Id.* at 14316, para. 69.

[325] *Supply Chain 3rd R&O,* 36 FCC Rcd at 11965, para. 19.

[326] *Id.* at 11965-66, 11967, 11969-71, paras. 20, 23, 29-30.

[327] *See March 2021 Covered List Public Notice* at 2 and n.12 (specifically citing section 889(f)(3) of the 2019 NDAA). Following the Commission's 2020 decision in the *Supply Chain 2nd R&O* to include this equipment on the Covered List, *see Supply Chain 2nd R&O*, 35 FCC Rcd at 14315-16, para. 67, and the Commission's inclusion of this equipment on the Covered List in March 2021, the Commission received no petition for reconsideration challenging this inclusion.

[328] *See also March 2022 Covered List Public Notice*, Appendix; *September 2022 Covered List Public Notice*, Appendix.

[329] *Supply Chain 2nd R&O*, 35 FCC Rcd at 14290, para. 18; *Supply Chain 3rd R&O*, 36 FCC Rcd at 11965, 11985, paras. 19, 62; 47 CFR § 1.50004.

Hytera, Hikvision, and Dahua equipment) are on the current Covered List.[330] Finally, the Commission now requires that each advanced communications service provider file a report on an annual basis that identifies any "covered" equipment or service that was purchased, rented, leased, or otherwise obtained after August 14, 2018, or 60 days after new equipment or services are subsequently added to the Covered List.[331] Some providers, in their first annual reports, which were due in May of this year, identified certain "covered" equipment associated with their equipment or services, including various Huawei and ZTE network equipment (in their core, distribution, and access layers) and certain video surveillance equipment produced by Huawei (as well as produced by Hikvision and Dahua).[332] Providers submitting this report must certify to the accuracy of the information submitted.[333] In addition, the Commission's rules require that ETCs receiving universal service support certify that they do not use "covered" communications equipment and services produced by Huawei or ZTE.[334]

140. *Federal prohibitions under section 889 of the 2019 NDAA.* As we have noted, federal agency prohibitions also already have been adopted with regard to Huawei and ZTE equipment. Pursuant to section 889(a) of the 2019 NDAA, executive branch agencies are prohibited from procuring or otherwise obtaining certain "covered" telecommunications equipment, including equipment produced by Huawei or ZTE (or their subsidiaries/affiliates) under 889(f)(3)(A). Offerors of equipment for federal procurement are required to make representations as to whether they are offering "covered" Huawei or ZTE equipment as defined under section 889(f)(3)(A) of the 2019 NDAA.[335]

141. *Comments on prohibiting the authorization of "covered" Huawei and ZTE equipment.* The Commission received only a few comments that specifically addressed the proposed equipment authorization prohibition with respect to the particular equipment produced by either Huawei or ZTE. In comments submitted prior to adoption of the Secure Equipment Act of 2021, Huawei Cos. generally argue that the Commission lacked both legal authority and a factual basis for prohibiting authorization of such equipment under the Commission's equipment authorization program;[336] Huawei Cos. do not provide any specific discussion of the extent to which all or only some of its equipment is "covered" equipment. Huawei Cos. also assert that prohibiting authorization of Huawei equipment would not improve security in any meaningful way,[337] and further contend that such a prohibition would potentially have an adverse impact with regard to the global supply chain.[338] We note that ZTE has not filed any comments in this proceeding.

---

[330] *Supply Chain 2nd R&O*, 35 FCC Rcd at 14325-30, paras. 93-105; 47 CFR § 54.10.

[331] Secure Networks Act § 5. *See* 47 CFR § 1.50007(a) (in annual report, each advanced communications service provider must certify to the accuracy of the information submitted regarding covered communications equipment or services).

[332] This information is derived from staff review and analysis. Filers were required to identify equipment and services on the Covered List.

[333] 47 CFR § 1.50007(a).

[334] *Id.* § 54.11. As previously explained, the Commission aligned the scope of the certification requirement in section 54.11 of its rules to the scope of covered communications equipment and services eligible for reimbursement in the Reimbursement Program, which is communications equipment and services produced or provided by Huawei or ZTE. The certification requirement in section 54.11 of the Commission's rules goes into effect in 2023.

[335] *See* paragraph 13, *supra*.

[336] Huawei Cos. Comments at i.

[337] *Id.* at 7.

[338] *Id.* at 15.

142. The Coalition for a Prosperous America specifically supports prohibiting authorization of Huawei and ZTE equipment.[339] Commenting parties, however, generally do not focus their comments on the extent to which all of the Huawei or ZTE equipment should be deemed "covered" (although, as we discuss below, some commenters discuss Hytera, Hikvision, and Dahua equipment on this question). Several commenters, including TIA, China Tech Threat, JVC Kenwood, and Motorola comment broadly, supporting Commission action to block authorization of all the equipment identified in the Covered List produced by the named entities, including video surveillance equipment.[340] Others ask that the Commission provide clarity on what constitutes "covered" equipment, or make recommendations in that regard;[341] CTIA, for instance, asks in particular for clarity regarding whether handsets would be considered "covered" equipment.[342]

143. China Tech Threat also asserts that the Commission's proposal to prohibit authorization of equipment on the Covered List provides a way to go beyond other federal efforts that aim to address concerns relating to equipment that poses an unacceptable risk to national security (e.g., restricting federal procurement through the 2019 NDAA or mitigating the risk of installed devices).[343] Specifically, China Tech Threat asserts that the Commission's proposed regulation to prohibit future authorization of equipment on the Covered List does not duplicate other efforts and instead goes beyond those other efforts that do not "effectively address or mitigate the unacceptable risk of installed electronic equipment using radio frequencies."[344] It states that the 2019 NDAA restriction on federal procurement "leaves states, businesses, and individuals to purchase what they want, which unwittingly is unrestricted, vulnerable equipment."[345] China Tech Threat contends that the Commission's proposed regulation "reflects a clear, distinct mandate" from Congress to act, and would close the "loophole" created by the other efforts that have focused on the unacceptable risk in the federal procurement context.[346]

---

[339] Coalition for a Prosperous America Comments at 2. *See also* Hikvision USA Comments at 34 (stating that while all telecommunications equipment produce by Huawei or ZTE belongs on the Covered List, per the 2019 NDAA § 889(f)(3)(A), Hikvision's equipment, mentioned in § 889(f)(3)(B), which has a different statutory construction, does not).

[340] *See, e.g.*, TIA Comments at 5-6 (banning all equipment is a "logical outgrowth" of all the work that the Commission has been doing the past four years in the USF proceeding to "rip and replace" Huawei and ZTE equipment); China Tech Threat Comments at 45; JVC Kenwood USA Comments at 2; Motorola Reply at 2-3, 24 (supports Commission action to further ensure that equipment on the Covered List is not used in any U.S. network, asserting that public safety, law enforcement, critical infrastructure, and governmental networks should be afforded highest level of security by foreclosing use of such equipment; Commission should move promptly to adopt proposals to deny authorization to sell or market equipment on the Covered List).

[341] *See, e.g.*, NTCA at 5 (If the Commission chooses to use the equipment authorization process to prohibit covered equipment named on the Covered List, the Commission should be as clear as possible regarding the scope and limits of such bans); CTIA Comments at 18 (network equipment poses much different national security risks than consumer end devices, yet the *NPRM* treats them all equally with respect to the proposed changes to the equipment authorization regime); NCTA Comments at 16 (rather than a blanket prohibition for any importation, marketing, or sale of equipment on the covered list, the Commission could instead prohibit authorization for certain uses while preserving marketplace employment of such equipment in circumstances and contexts that do not implicate national security concerns).

[342] CTIA Comments at 11 (in seeking clarification, CTIA did not specify whether it was asking about handsets produced by any particular equipment producer named on the Covered List).

[343] China Tech Threat Reply at 10.

[344] *Id.*

[345] *Id.*

[346] *Id.* at 11.

(ii) Discussion

144. As proposed in the *NPRM*, we will prohibit from equipment authorization all equipment produced by Huawei and ZTE (as well as their subsidiaries and affiliates) that is on the Covered List. As identified pursuant to the Secure Networks Act and Congress's determination under section 889(f)(3) of the 2019 NDAA, such equipment includes both "telecommunications equipment" and "video surveillance equipment" produced by these two entities (and their subsidiaries and affiliates). Specifically, Congress defines "covered telecommunications equipment or services" in section 889(f)(3)(A) as "telecommunications equipment" produced by Huawei and ZTE,[347] and in section 889(f)(3)(C) Congress included "telecommunications or video surveillance services provided" by Huawei or ZTE "or using such *equipment* (emphasis added)."[348] Combining the equipment identified by Congress in sections 889(f)(3)(A) and (C), the Covered List published by PSHSB states that "covered" equipment under the Secure Networks Act includes "[t]elecommunications equipment" produced or provided by Huawei or ZTE, "including telecommunications or video surveillance services produced or provided by such entity using such equipment."[349] The Commission was required to place this equipment on the Covered List, and had no discretion not to do so.[350] As the Commission has explained, the Secure Networks Act requires the Commission to accept and incorporate on the Covered List the determinations as provided, and should interested parties seek to reverse or modify the scope of one of these determinations, the party should petition the source of the determination.[351] We further note that the Congress in the Secure Equipment Act, with its direct reference to this rulemaking, in which the Commission expressly proposed to prohibit authorization of the "telecommunications equipment" and "video surveillance equipment" specified on the Covered List,[352] endorsed inclusion of this equipment on the Covered List as equipment that must not be authorized by the Commission.[353]

145. In addition, as explained in the *Supply Chain 2nd R&O* and *Supply Chain 3rd R&O*, the Commission need not make any Secure Networks Act §2(b)(2) "capability" assessment of the Huawei or ZTE equipment, under either §2(b)(2)(A) or (B) of the Secure Networks Act, since, in effect, we find that Congress under §889(f)(3) of the 2019 NDAA has made that capability determination regarding this equipment, i.e., that it "otherwise pos[es] an unacceptable risk" to national security, pursuant to §2(b)(2)(C).[354] Thus, for purposes of the prohibition that we are adopting in this proceeding, "covered" equipment includes "telecommunications equipment" and "video surveillance equipment" produced by Huawei and ZTE.

146. In section III.C.5, below, we provide additional Commission guidance and explanation about what equipment constitutes covered "telecommunications equipment" and "video surveillance equipment" for purposes of the prohibition on such equipment authorization.

---

[347] 2019 NDAA § 889(f)(3)(A). As we discuss below, Congress in section 899(f)(3) also identified equipment produced by Hytera, Hikvision, and Dahua. 2019 NDAA § 889(f)(3)(B) and (C).

[348] 2019 NDAA § 889(f)(3)(C).

[349] *See March 2021 Covered List Public Notice* (Appendix); *March 2022 Covered List Public Notice* (Appendix); *September 2022 Covered List Public Notice* (Appendix).

[350] *Supply Chain 2nd R&O*, 35 FCC Rcd at 14315-16, paras. 67, 69, 71; *see id.* at 14320, para. 80; *Supply Chain 3rd R&O*, 36 FCC Rcd at 11965, para. 19.

[351] *Supply Chain 2nd R&O*, 35 FCC Rcd at 14324, para. 89.

[352] *NPRM*, 36 FCC Rcd at 10596, para. 40.

[353] Secure Equipment Act, § 2(a)(2) (mandating that the Commission clarify that it will no longer approve any application for equipment authorization for equipment that is on the Covered List published pursuant to the Secure Networks Act).

[354] *Supply Chain 2nd R&O*, 35 FCC Rcd at 14315-16, para. 67.

b. "Covered" equipment produced by Hytera, Hikvision, and Dahua

(i) Background

147. *The Secure Networks Act and section 889(f)(3) of the 2019 NDAA.* As discussed above, pursuant to the Secure Networks Act section 2(c)(3) and section 889(f)(3)(B) and (C), PSHSB placed equipment produced by Hytera, Hikvision, and Dahua on the Covered List on March 12, 2021,[355] and this equipment remains on each subsequently updated Covered List.[356] In particular, regarding these three entities the 2019 NDAA states that "covered telecommunications equipment and services" means:

> (B) For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities).
> (C) Telecommunications or video surveillance services provided by such entities or using such equipment.[357]

148. *Commission interpretation of "covered" equipment under section 889(f)(3)(B) and (C).* In the *Supply Chain 2nd R&O*, the Commission discussed Congress's section 889(f)(3)(B) and (C) determinations with respect to Hytera, Hikvision, and Dahua "video surveillance and telecommunications" equipment. In particular, it examined whether Congress' determinations in these two provisions required the Commission, pursuant to the Secure Networks Act, to place such equipment among the "communications equipment" to be included on the Covered List.[358] The Commission concluded that Congress's § 889(f)(3)(B) and (C) determinations indeed did require the Commission to incorporate onto the Covered List "video surveillance and telecommunications equipment" produced by these three entities and capable of the function outlined in section 2(b)(2)(A), (B), or (C) of the Secure Networks Act.[359] In addition, consistent with its proposal in its 2020 *Supply Chain 2nd Further Notice*,[360] the Commission further stated that it would incorporate into the Covered List such equipment produced by Hytera, Hikvision, and Dahua "to the extent it is used for public safety or security."[361]

149. *The current Covered List.* Regarding Hytera, Hikvision, and Dahua, the current Covered List states, as it has since it was initially published on March 12, 2021, that "covered" equipment includes: "[v]ideo surveillance and telecommunications equipment produced or provided by" Hytera, Hikvision, or Dahua, "to the extent used for the purpose of public safety, security of government facilities, physical surveillance of critical infrastructure, and other national security purposes, including

---

[355] *March 2021 Covered List Public Notice* at 2 and n.12 (specifically citing section 889(f)(3) of the 2019 NDAA). Appendix.

[356] *March 2022 Covered List Public Notice*, Appendix; *September 2022 Covered List Public Notice*, Appendix.

[357] 2019 NDAA § 889(F)(3)(A), (C).

[358] *Supply Chain 2nd R&O*, 35 FCC Rcd at 14315-16, paras. 66, 68-69 (citing *Supply Chain 2nd Further Notice*). In the underlying *Supply Chain 2nd Further Notice*, the Commission had expressly asked whether video surveillance equipment produced by Hytera, Hikvision, and Dahua qualify as "communications equipment" for purposes of the Secure Networks Act. *Supply Chain 2nd Further Notice*, 35 FCC Rcd at 7832, para. 35.

[359] *Supply Chain 2nd R&O*, 35 FCC Rcd at 14316, para. 68.

[360] *Supply Chain 2nd Further Notice*, 35 FCC Rcd at 7832, para. 35.

[361] *Supply Chain 2nd R&O*, 35 FCC Rcd at 14316, para. 68 (citing *Supply Chain 2nd Further Notice*).

telecommunications or video surveillance services produced or provided by such entit[ies] or using such equipment."[362]

150. *Commission prohibitions and other requirements concerning Hytera, Hikvision, and Dahua "covered" equipment.* The Commission has adopted and implemented certain requirements that apply specifically to Hytera, Hikvision, and Dahua equipment. The Commission prohibits the use of any Federal subsidy administered by the Commission for support for advanced communications services to purchase, rent, lease, or otherwise obtain any "covered" communications equipment or services on the Covered List, which includes such equipment produced by Hytera, Hikvision, and Dahua.[363] Also, the Commission requires that advanced communications service providers report such "covered" equipment in their networks, and in the first annual reports filed in May 2022 some have indicated that their networks and services include certain "covered" equipment produced by these entities.[364]

151. *Federal procurement prohibitions.* With regard to the federal agency prohibition on "covered" equipment under section 889 of the 2019 NDAA, executive branch agencies are prohibited from procuring or otherwise obtaining certain "covered" telecommunications equipment, including certain equipment produced by Hytera, Hikvision, and Dahua (or their subsidiaries/affiliates) under 889(f)(3)(B). As noted above, in 2020 the GSA Supply Chain Risk Management (SCRM) Review Board provided guidance criteria for evaluating the applicability of the procurement prohibition relating to "covered" equipment, including Hytera, Hikvision, and Dahua equipment.[365] In particular, it provided criteria associated with its interpretation of section 889(f)(3)(B) that can be used to determine whether the prohibition applies; per its "decision tree," the prohibition on video surveillance and telecommunications equipment produced by Hytera, Hikvision, and Dahua applies if the purposes of the use of that technology is for public safety, security or government facilities, physical surveillance of critical infrastructure, or other national security purpose.[366]

152. *Comments on scope of "covered" equipment with regard to Hikvision, Dahua, and Hytera.* The Commission received extensive comment and *ex parte* submissions regarding whether any Hikvision, Dahua, or Hytera equipment constitutes "covered" equipment in the first instance, as well as on the extent to which the Commission should prohibit authorization of any equipment produced by these entities in the Commission's equipment authorization program.

153. Hytera Ltd. and Hytera US, Hikvision USA, and Dahua USA each contend that its equipment generally is not "covered" equipment under the Secure Networks Act and 2019 NDAA section 889(f)(3), does not belong on the Covered List, and accordingly should not be prohibited from obtaining equipment authorizations.[367] Hytera US notes that Hytera equipment has a significant presence in the land

---

[362] *2022 Covered List Public Notice* (Appendix); *see March 2022 Covered List Public Notice* (Appendix); *March 2021 Covered List Public Notice* at 2 and n.12 (specifically citing section 889(f)(3) of the 2019 NDAA) & Appendix. Following the Commission's 2020 decision in the *Supply Chain 2nd R&O* to include this equipment on the Covered List, *see Supply Chain 2nd R&O*, 35 FCC Rcd at 14316, para. 68, and the Commission's inclusion of this equipment on the Covered List in March 2021, the Commission received no petition for reconsideration challenging this inclusion on the Covered List of "telecommunications equipment" or "video surveillance equipment" produced by these entities.

[363] *Supply Chain 2nd R&O*, 35 FCC Rcd at 14325-30, paras. 93-105; 47 CFR § 54.10. This prohibition also applies to Huawei and ZTE equipment.

[364] This information was supplied the Commission was provided in reports filed with the Commission.

[365] *See, e.g.*, "SCRM Criteria for Section 889 Part A" and "SCRM Criteria for Section 889 Part B," respectively, found at https://www.gsa.gov/cdnstatic/SCRM%20review%20board%20889%20PART%20A%20Rubric_0.pdf; https://www.acquisition.gov/FAR-Case-2019-009/889_Part_B.

[366] *See* https://www.acquisition.gov/FAR-Case-2019-009/889_Part_B.

[367] As noted above, no representatives of Hytera, Hikvision, or Dahua filed a petition for reconsideration challenging inclusion of their respective equipment on the Commission's Covered List in March 2021 when that list first

(continued….)

mobile radio equipment industry in the United States, and that its equipment also includes body-worn cameras.[368] As Hikvision and Dahua representatives note, their equipment has a significant presence in the video surveillance equipment market in the United States.[369] All three companies also produce other types of equipment as well,[370] much of which has obtained equipment authorizations from the Commission through the years. Each asserts that its equipment does not pose any risk to national security.[371] In addition, many other commenters, including businesses that sell Hytera, Hikvision and Dahua equipment to a wide range of customers (e.g., individual consumers, schools, manufacturers, medium-sized and small businesses, hospitals), oppose action by the Commission to prohibit authorization of these companies' equipment, contending that the equipment is secure and poses no threat, and serves customers well often at less expense.[372] Hikvision USA and Dahua USA also contend that nothing in the Secure Equipment Act of 2021 expands the scope or category of devices that are "covered" under the Secure Networks Act or section 889(f)(3) of the 2019 NDAA with respect to the instant proceeding.[373]

154. In their several filings, Hytera Ltd. and Hytera US, Hikvision, and Dahua generally make two sets of arguments. The first concerns the scope of "covered" equipment based on their readings of the Secure Networks Act and its definition of "communications equipment" and the "capability"

---

included, as "covered" equipment, "telecommunications equipment" or "video surveillance equipment" produced by them.

[368] Hytera US Comments at 3 (Hytera products includes handsets, repeaters, trunking systems, private land mobile radios (PLMR) and digital mobile radios (DMR), body-worn cameras, and private systems tailored to customers' needs; it states that equipment users include a range of sectors, including government, local public utilities, taxi companies, delivery services, towing companies, hotels, restaurants, large department stores, and schools and universities).

[369] *See, e.g.*, Hikvision USA Comments at 1, 7-8, 15-19 (Hikvision is a global video surveillance company whose products include video security systems that American companies use to protect their personnel and property; it has a market share of 14.3% in the video surveillance market in the United States); Dahua USA Comments at 2 (Dahua products offer "end-to-end security solutions, systems, and services" for city operations, corporate management, and consumers); Dahua USA Jan. 4, 2022 *Ex Parte* at 3 (Dahua mainly markets in the United States products that include video cameras (including IP, composite video interface, and Wi-Fi cameras), video recorders (including IP and composite video interface recorders), and pan-tilt-zoom cameras).

[370] *See, e.g.*, Hikvision USA Comments at 16 n.17 (while cameras and network video recorders make up a majority of its products sold in the United States, Hikvision also produces other product lines including access control devices, video intercom devices, security radar, encoder/decoders, digital signal boxes, ethernet switches, monitors, and accessories); Hikvision Nov. 22, 2021 *Ex Parte* at 2 (Hikvision products do not include broadband network equipment such as network switches or routers, cell network infrastructure, or gateway routers); Dahua USA Comments at 2 (Dahua also offers a range of other products, including cables, displays, power supplies, alarm sensors, storage devices, intercoms, and access control solutions); Dahua USA Jan. 4, 2022 *Ex Parte* at 3 (Dahua's products in the United States include access control systems, intercom systems, switches that perform connections between video cameras and recorders deployed by end-users (but not switches that are used in telecommunications networks or the provision of advanced communications services), monitors, and accessories); Hytera US Comments at 3 (Hytera makes handsets, repeaters, and trunking systems, and develops and markets wireless two-way radios and private systems tailored to its customers' needs).

[371] *See, e.g.*, Hikvision USA Reply Comments at 8-14; Dahua USA Comments at 15; Hytera US Comments at 16.

[372] *See, e.g.*, ENS Security Comments at 1; Chown Hardware Comments at 1; Computer Supporter & Associate Comments at 1; Gen Net, Inc. Comments at; Baker's Communications Comments at 1; Diversified Communications Group at 1; Metrotalk Comments at 1.

[373] *See, e.g.*, Hikvision USA Nov. 22, 2021 *Ex Parte* at 2 (Secure Equipment Act did not expand devices to be listed on the Covered List); Hikvision USA Apr. 7, 2022 *Ex Parte* at 5-6 (Secure Equipment Act does not expand the category of products for which the Commission may deny equipment authorizations); Hikvision USA May 27, 2022 *Ex Parte* at 1, 5 (Secure Equipment Act and Secure Network Act do not cover Hikvision equipment); Dahua USA Dec. 10, 2021 *Ex Parte* at 2; Dahua USA Jan. 4, 2022 *Ex Parte* at 2.

requirement, which they contend would preclude the equipment that they respectively produce, including video surveillance and land mobile radio equipment, from being deemed "covered." Indeed, each of the three generally contend that its equipment in the United States does not fall within this definitional and capability scope of the Secure Networks Act, and thus is not "covered."[374] On these grounds, they each contend that their equipment never should have been placed on the Covered List in the first instance (in March 2021) and request that the Commission now proceed to remove their equipment from the Covered List.[375] The second set of arguments made by representatives of these three companies focuses on the scope of equipment that is "covered" equipment under section 889(f)(3)(B) of the 2019 NDAA. They contend that, because of what they term as a "use" requirement in § 889(f)(3)(B) related to "covered" equipment, the Commission does not have a basis for categorically excluding authorization of any of their equipment used for other purposes.

155. In response, Motorola counters that the Commission should reject the arguments of Hytera, Hikvision, and Dahua that the Commission should now remove their respective equipment from the Commission's Covered List or otherwise find that their equipment does not fall within the scope of "covered" equipment under the Secure Networks Act (addressing arguments concerning whether the equipment is "communications equipment" or must be interconnected).[376] Motorola also contends, contrary to views of Hytera, Hikvision, and Dahua representatives, that 2019 NDAA section 889(f)(3)(B) provision and the "covered" equipment on the Covered List supports the Commission taking action to prohibit authorization of any of their equipment.[377] Motorola asserts broadly that their equipment poses a threat to the United States.[378]

156. IPVM specifically supports Commission action to prohibit authorizing their video surveillance equipment, contending that the equipment includes vulnerabilities that would allow hackers to access camera feeds and recordings, switch devices on and off, reposition cameras, hack into the networks in which they are connected, or use the devices in a botnet attack.[379] It contends that these companies and their equipment pose a threat to national security, and states that the vast majority of their cameras fall into the category of "Internet protocol (IP) cameras" that are designed to be used with the internet and a titular feature of these devices, consistent with what end users expect from surveillance products,[380] and that some of Hikvision's current cameras require an internet connection.[381] Hikvision USA counters IPVM, stating that there is no basis for concluding that Hikvision's video surveillance equipment poses any unique or material cybersecurity threat either to U.S. infrastructure or American businesses or end users, and further states that it remains the end user's responsibility to protect its

[374] Hikvision USA Nov. 17 *Ex Parte* at 1 (Hikvision's equipment, specifically including its video surveillance cameras and network video recorders, is not "communications equipment" that is "essential to broadband service," and "the Commission is statutorily compelled to remove Hikvision from the Covered List"); Dahua USA Reply Comments at 13 (none of the Dahua equipment is "communications equipment" under the Secure Networks Act, and therefore none of its equipment mentioned on the Covered List can be prohibited from receiving an equipment authorization); Hytera Ltd. Aug. 17, 2021 *Ex Parte* at Slides 11-13 (the Secure Networks Act is directed to broadband equipment, and Hytera land mobile and digital mobile radio equipment is categorically not included).

[375] *See, e.g.*, Hikvision USA Nov. 17, 2021 *Ex Parte* at 1; Dahua USA May 9, 2022 *Ex Parte* at 4; Hytera Ltd. Aug. 17, 2021 *Ex Parte*, Slides at 15.

[376] Motorola May 2, 2022 *Ex Parte* at 4-7.

[377] Motorola May 2, 2022 *Ex Parte* at 7.

[378] Motorola Reply at 19-24.

[379] IPVM Comments at 1-3. IPVM states that it is a research organization focused on surveillance businesses and technologies, and that it has issued reports on Hikvision and Dahua equipment and activities over the past decade. *Id.* at 1. IPVM also asserts that the People's Republic of China has access to these vulnerabilities. *Id.* at 2.

[380] IPVM Reply at 1-3 (contending that these companies are not trustworthy).

[381] IPVM Reply at 7.

equipment.[382] As noted above, several other commenters – including TIA, China Tech Threat, Coalition for a Prosperous America, JVCKenwood, and NCTA – generally support Commission action to prohibit authorization of "covered" equipment without focusing their comments specifically on equipment produced by the particular entities named on the Covered List.[383] And, as discussed above, China Tech Threat also endorses the Commission's proposal to prohibit authorization of equipment on the Covered List as a way to go beyond other federal efforts that aim to address concerns relating to equipment that poses an unacceptable risk to national security (e.g., restricting federal procurement through the 2019 NDAA or mitigating the risk of installed devices),[384] contending the prohibiting authorization of the equipment closes a loophole that would otherwise leave states, businesses, and individuals to unwittingly purchase vulnerable equipment.[385]

(ii) Discussion

157. We first address the various arguments regarding whether "telecommunications equipment" and "video surveillance equipment" produced by Hytera, Hikvision, and Dahua falls within the scope of "covered" equipment under the Secure Networks Act section 2(c)(3) and the determination by Congress under section 889(f)(3)(B) and (C) of the 2019 NDAA concerning those companies' equipment, and belongs on the Covered List. In our decision, we explain that their "telecommunications equipment" and "video surveillance equipment" was previously determined to be "covered" and has accordingly been placed on the Covered List. We then address the extent to which the Commission can, through its equipment authorization program, prohibit authorization of any of the "video surveillance equipment and telecommunications equipment" produced by these companies (or their respective subsidiaries and affiliates). We conclude that we will prohibit in our equipment authorization program authorization of such equipment produced by Hytera, Hikvision, and Dahua "for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes."

158. We note that while this section focuses on the overall scope of what constitutes "covered" equipment on the Covered List, in section III.C.5 below, we provide further Commission guidance regarding what types of equipment constitutes "telecommunications equipment" and "video surveillance equipment" that will be prohibited from obtaining authorization under the Commission's equipment authorization program.

(a) "Covered" equipment includes certain "video surveillance and telecommunications equipment" produced by these entities

159. *Background.* As discussed above, Hytera, Hikvision and Dahua each contend that the Secure Networks Act requires that the Commission's Covered List now remove listing their "video surveillance and telecommunications equipment" as "covered," and that in any event the Commission should now preclude their equipment from being deemed "covered" and not prohibit authorization of that

[382] *See, e.g.*, Hikvision USA Feb. 23, 2022 *Ex Parte* at 1-4.

[383] *See, e.g.*, TIA Comments at 10 (FCC clearly has a substantial record from agencies with national security expertise, as well as the President and acts of Congress, demonstrating the security risks posed by the covered entities); China Tech Threat at 45-46 (supports the FCC denying all future equipment authorizations from the five entities of the FCC's Covered List as well as to revoke past authorizations); Coalition for a Prosperous America Comments at 2 (restricting equipment from Huawei and Covered List entities will improve market competition, restore American jobs, and improve equipment security by removing PRC from the supply chain); JVCKenwood at 2 (Commission should prohibit the authorization of equipment manufactured by covered entities); NCTA at 4 (supports the Commission's goal of prohibiting the importation, marketing, and sale of insecure devices from companies such as Huawei and ZTE that appear on the covered list).

[384] China Tech Threat Reply at 10.

[385] *Id.*

equipment in the instant proceeding. We discuss their extensive arguments, as well as Motorola's counter-arguments, before addressing our conclusions below.

160. In their presentations, Hytera Ltd., Hytera US, and PowerTrunk make similar arguments, albeit it more focused on Hytera equipment such as its two-radio land mobile radio/digital mobile radio (LMR/DMR) equipment. Consistent with arguments made by Hikvision and Dahua representatives, they generally contend that Hytera equipment should be excluded from the Commission's Covered List because such equipment does not meet either the definitional requirements of what constitutes "communications equipment" under the Secure Networks Act, or that Act's "capability" requirements associated with what constitutes "covered" communications equipment insofar as that equipment is not capable either of routing or redirecting user traffic or permitting visibility into user data packets.[386] They also assert that all of Hytera's products in the U.S. are consumer premises equipment (CPE), and that because such equipment does not fall within the Communications Act's definition of "telecommunications equipment" it should not be deemed "telecommunications equipment" under the Secure Networks Act.[387] Further, Hytera US states that its particular LMR/DMR equipment, which operates under private land mobile regulations for use on private systems, is not generally designed to be interconnected with the public switched network or any internet or broadband network, and cannot on its own provide "advanced communications services" such as broadband services (i.e., at 200 kbps).[388] PowerTrunk's separate submission focuses on its advanced DMR TETRA technology, which it states is used by utility and transportation industries as well as state and federal agencies, including the New Jersey Transit Corporation (NJTC)). Power Trunk asserts that this equipment should not be "covered" because the Committee for Foreign Investment in the United States (CFIUS) investigated this technology and in 2018 issued a Letter of Assurance (LOA) that authorized sale of the equipment in the United States, and because the Commission determined in its *Supply Chain 2nd R&O* to rely on specific determinations made by executive branch agencies such as CFIUS regarding national security concerns.[389] Finally, Hytera asks that the Commission clarify its Covered List to make the "capability" requirement clearer in order to eliminate confusion as to whether Hytera equipment is "covered."[390]

161. Regarding video surveillance equipment, Hikvision USA and Dahua USA each contend that its equipment is not "covered" "communications equipment" as required and defined under the Secure Networks Act (sections 2(b) and 9) insofar as its equipment is not core "network" equipment (either telecommunications or internet infrastructure) but instead only involves "peripheral" or "incidental" devices that are not "essential to the provision of advanced communications service" that is statutorily required for "covered" equipment under the Secure Networks Act.[391] Noting that the

---

[386] *See, e.g.*, Hytera US Comments at ii, 10-11; Hytera Ltd. Aug. 17, 2021 *Ex Parte* at 1-2. *See, e.g.*, Hytera US Comments at ii, 10-11; Hytera Ltd. Aug. 17, 2021 *Ex Parte* at 1-2.

[387] Hytera Ltd., Hytera USA, and PowerTrunk June 3, 2022 *Ex Parte* at 2. *See also* Hytera Ltd., Hytera USA, and PowerTrunk Aug. 17, 2021 *Ex Parte*, Slide Presentation at 8 (citing section 153(22) of the Communications Act of 1934, as amended (defining the term "telecommunications equipment" as meaning equipment, other than customer premises equipment, used by a carrier to provide telecommunications services).

[388] Hytera US Comments at ii, 11-12; Hytera Ltd. Apr. 1 *Ex Parte* at 2. Hytera Ltd. states that manufacturers applying for equipment authorizations are in the best position to make this technical analysis, which can be validated by TCBs. Hytera Communications Corporation Reply at 5-6.

[389] PowerTrunk Comments at 2-3. In its comments in this proceeding, NJTC urges the Commission to ensure that: (1) the adopted rules amend the Covered List to explicitly exempt businesses that have received a LOA from CFIUS, and (2) clarify that exempt radio equipment should be permitted to stay in use in perpetuity. NJTC Comments at 1-2 (noting the LOA and requesting that the Commission clarify that equipment in the LOA should be exempted from the proposed prohibition on "covered" equipment).

[390] Hytera US Comments at iii, 4, 6, 9-11.

[391] *See, e.g.*, Hikvision USA Comments at 1-3 (citing Secure Networks Act, sections 2(b) and 9); Hikvision USA Nov. 22 *Ex Parte* at 2; Hikvision USA Apr. 7 *Ex Parte* at 5-6; Dahua USA Reply at 11-13 (video monitoring is not (continued….)

Commission subsequently further defined "communications equipment" as "all equipment … used *in* fixed and mobile broadband networks" (emphasis added),[392] Hikvision contends that its cameras and video network recorders, even though they may connect to such networks, are neither "essential" to the provision of telecommunications service nor "used in" the networks, and thus are not "communications equipment."[393] Hikvision USA and Hytera US also assert that their respective equipment does not constitute "covered" equipment because it does not meet the "capability" requirements of section 2(b) of the Secure Networks Act insofar as it is not generally capable of "routing or redirecting user data traffic" or "permitting visibility into any user data"[394] or "causing the network to be disrupted remotely."[395] In this vein, Hikvision USA and Dahua USA also claim that the Internet of Things (IoT) equipment and other CPE that they produce falls outside of the scope of the Secure Networks Act.[396] Hikvision USA and Dahua USA also state that most of their equipment (including their video surveillance equipment) can be, and frequently is, set up in configurations not connected to the internet, and accordingly that such equipment is not "covered" and thus should not be subject to prohibition from equipment authorizations.[397] Hikvision USA further asserts that even if "communications or telecommunications service" could include video surveillance equipment, it cannot include equipment that is not video surveillance equipment.[398]

162. In response, Motorola argues as a preliminary matter that the Commission should reject any argument to remove the listing of their equipment from the Covered List, contending that Hytera, Hikvision and Dahua representatives are precluded from requesting this because they each failed to challenge the Commission's 2020 *Supply Chain 2nd R&O* that named their equipment as "covered"

"essential" to the provision of advanced communications services, but is purely "incidental" to it); Dahua USA Jan. 4 *Ex Parte* at 3.

[392] Hikvision USA Comments at 38 (referencing the *Supply Chain 2nd R&O*, para. 52).

[393] *Id.* at 38-39.

[394] *See, e.g.*, Hikvision USA Comments at 3; Hytera US Comments at 10-11.

[395] *See, e.g.*, Hikvision USA Nov. 17, 2022 *Ex Parte* at 9.

[396] *See, e.g.*, *Id.* at 5 (handsets and other customer premises equipment, including IOT devices that utilize advanced communications services, are distinctly different from core networks, and therefore not "covered"); Dahua USA January 4, 2022 *Ex Parte* at 2 (Commission is neither authorized to exclude all Dahua equipment from the equipment authorization process under part 2 of the Commission's rules, nor to subject Dahua USA's peripheral Internet of Things non-communications equipment to discriminatory treatment under those rules.) Hikvision USA argues, in particular, that the Commission in its *Supply Chain 3rd R&O* acknowledged that handsets and other consumer premises equipment, including IOT devices – the types of devices that Hikvision contends include its video surveillance equipment – are used to access and utilize advanced communications services but are distinctly different from cell sites, backhaul, and core network. Hikvision USA Nov. 17 *Ex Parte* at 4-5 (citing *Supply Chain 3rd R&O*, 36 FCC Rcd at 11996, para. 94).

[397] *See, e.g.*, Hikvision USA Comments at 7-12 (noting that its cameras can be deployed by end users in several ways, including: as a standalone physically isolated deployment, a logically-separated deployment, or, if the end-users so chooses, directly connecting to the internet); Hikvision USA Nov. 22 *Ex Parte*, Slides at 7-9 (same); Dahua USA Comments at 21 (significant amount of Dahua equipment used in the United States is used in a closed network environment entirely disconnected from the broader public network); Dahua USA Reply at 4-6 (common configurations by end users are: deployment of Dahua devices on a physically isolated network such as a local area network outside of the internet, deployment over an internal network that is interconnected with the internet are logically separated from other devices (and end user may employ a firewall); or deployment in which the equipment is interconnected to the public network that enable updates (e.g., software/firmware updates) and/or enable the end-user to have remote access). With regard to remote monitoring or managing of a video surveillance, both explain three general methods – use of a virtual private network, use of a cloud-based access model, or port-forwarding by the end-user. *See, e.g.*, Hikvision USA Comments at 12-13; Dahua USA Reply at 5-6.

[398] Hikvision USA Nov. 17, 2022 *Ex Parte* at 6-7 (citing thermal monoculars and handheld temperature screening products as such examples); Hikvision USA May 27 *Ex Parte* at 5.

equipment on the basis of the 2019 NDAA's § 889(f)(3)(B) determination,[399] (which was followed by PSHSB's inclusion of their equipment on the Covered List in March 2021). In more recent filings, Motorola cites the Hobbs Act as another basis for precluding the three companies from making those arguments for removal from the Covered List.[400]

163. Motorola also counters arguments by Hytera, Hikvision, and Dahua representatives that their telecommunications and video surveillance equipment does not fall within the scope of the Secure Networks Act on the grounds that it is not "communications equipment" that is "essential" to the provision of advanced communications service. Taking the opposite view, Motorola points to the Commission's interpretation of "communications equipment or service" under the Secure Networks Act as meaning "any equipment or service used in fixed or mobile networks that provides advanced communication service," and contends that any equipment that can be used in a fixed or mobile broadband network to enable "users to originate and receive high quality voice, data, graphics, and video telecommunications using any technology with connection speeds of at least 200 kbps in either direction" would satisfy this definition.[401] In Motorola's view, when a customer operates a Hytera radio or Hikvision camera utilizing a broadband service, such equipment would be "used" in a fixed or mobile broadband network and thus would constitute "communications equipment or service" for purposes of inclusion on the Covered List.[402] Motorola argues that to be included on the Covered List does not require that their equipment be interconnected since it could be interconnected,[403] and that the equipment need not be capable of routing or redirecting user data traffic or permit visibility into any user data or packets because Congress specifically identified their equipment as "covered" equipment in section 889(f)(3) of the 2019 NDAA.[404]

164. Motorola also disagrees with the view that telecommunications or video surveillance equipment produced by the three companies does not fall within the scope of "communications equipment" because broadband service providers themselves do not use such equipment in providing advanced telecommunications service; Motorola instead contends that, when considering whether equipment falls within the scope of "covered" equipment under the Secure Networks Act, there is no requirement that the provider of the advanced communication service must itself be the "user" of the telecommunications or video surveillance equipment included on the Covered List, given that the network security threat posed by the equipment used in a fixed or mobile broadband network does not depend upon the identity of the user.[405] Motorola argues that, regardless of the entity enabling the equipment (e.g., Hytera's LMR or Hikvision's video surveillance equipment) that connects to the internet, such equipment raises security risks about which Congress was concerned when enacting the Secure Networks Act.[406] Further, Motorola disagrees with any contention that, in order to be placed on the Covered List, the equipment must actually be "used" in a fixed or mobile broadband network. Instead, Motorola asserts that to be included on the Covered List it is sufficient that the equipment be capable of being "used" in a

---

[399] Motorola Reply Comments at 10.

[400] *See, e.g.*, Motorola Mar. 24, 2022 *Ex Parte* at 2-3 (the Commission placed video surveillance and telecommunications equipment produced by Hytera, Hikvision, and Dahua on the Covered List, per in its December 2020 *Supply Chain 2nd R&O* following notice and comment, and these parties did not challenge that order and under the Hobbs Act should now be found to be precluded from collaterally attacking that decision).

[401] *Id.* at 4 (emphasis added by Motorola); *see* Motorola Reply at 13 (contending that interconnection is not required, but noting that that in any event Hytera and Hikvision equipment can interconnect).

[402] Motorola Mar. 24, 2022 *Ex Parte* at 4; Motorola May 3, 2022 *Ex Parte* at 5.

[403] Motorola Reply at 1-11.

[404] *Id.* at 10-11 (stating that the Commission had already rejected arguments that 2019 NDAA section 889(a)(2) limitations applied to section 889(f)(3), citing the *Supply Chain 2nd R&O*, 35 FCC Rcd at 14315, para. 67).

[405] Motorola May 3, 2022 *Ex Parte* at 5.

[406] Motorola Reply at 13; *see also* Motorola May 3, 2022 *Ex Parte* at 5.

fixed or mobile broadband network, and that any other reading would be administratively unworkable and would circumvent Congressional intent by removing equipment from the Covered List that poses an unacceptable risk based on a particular customer's use of their equipment.[407] Motorola also disagrees with PowerTrunk that its equipment should not be prohibited from authorization because that equipment has been marketed for sale to public safety and critical infrastructure entities.[408]

165. Finally, Motorola also urges the Commission to reject any argument that use of the word "telecommunications equipment" in the 2019 NDAA should be interpreted as defined in the Communications Act, stating that the NDAA could have but did not reference the Communications Act; Motorola argues that the statutory scheme of the NDAA is different, and there is no indication that Congress intended that the term have the same meaning as the statute, and that the Commission should construe the term in the NDAA expansively, consistent with the national security policies underlying section 889.[409]

166. *Discussion.* Following review of the extensive arguments presented by Hytera, Hikvision, and Dahua representatives, we reject their contentions that the equipment that they produce cannot constitute covered communications equipment under the Secure Networks Act and section 889(f)(3) of the 2019 NDAA, and that it does not belong the Commission's Covered List. Accordingly, we reject arguments by these companies that the Commission now should remove "video surveillance and telecommunications equipment" produced by these entities (or their subsidiaries or affiliates) from the Covered List.

167. First, in the Secure Networks Act section 2(c)(3) and section 889(f)(3) of the 2019 NDAA, Congress identified as covered communications equipment "video surveillance and telecommunications equipment" produced by these entities (and any of their subsidiaries or affiliates). We note that in its 2020 decision in the *Supply Chain 2nd R&O* the Commission already concluded that, pursuant to the Secure Networks Act and its incorporation of section 889(f)(3) of the 2019 NDAA, "telecommunications equipment" and "video surveillance equipment" produced by Hytera, Hikvision and Dahua is "covered" communications equipment under the Secure Networks Act,[410] and as a result PSHSB properly placed this equipment on the Covered List when it first published the list in March 2021. Accordingly, we reject arguments by these companies that the Commission now should remove inclusion of "video surveillance and telecommunications equipment" produced by these entities (or their subsidiaries or affiliates) from the Covered List.

168. The Secure Networks Act expressly provides in section 2(c) that the Commission must place on the Covered List any communications equipment that poses an unacceptable risk to the national security or the security and safety of United States persons "based solely on one or more" of the determinations made by four enumerated sources specified in the Act.[411] Specifically, one of those determinations, set forth in section 2(c)(3) of the Secure Networks Act, provides the following on determination relating to communications equipment posing an unacceptable risk: "[t]he communications equipment or service being covered telecommunications equipment or services, as defined in section 889(f)(3)" of the 2019 NDAA.[412] In turn, section 889(f)(3), which was enacted prior to the Secure Networks Act, provides that "[c]overed telecommunications equipment or services" includes "telecommunications equipment" and "video surveillance equipment" produced by Hytera, Hikvision,

[407] *See, e.g.*, Motorola Mar. 24, 2022 *Ex Parte* at 4-5.

[408] Motorola June 17, 2022 *Ex Parte* at 2-3.

[409] Motorola Reply at 12-13; *see also* Motorola May 27, 2022 *Ex Parte* at 2.

[410] *Supply Chain 2nd R&O*, 35 FCC Rcd at 14316, paras. 68-69.

[411] Secure Networks Act § 2(c).

[412] *Id.* § 2(c)(3).

and Dahua, per section 889(f)(3)(B),[413] as well as "[t]elecommunications or video surveillance services provided by such entities or *using such equipment*," per section 889(f)(3)(C) (emphasis added). Given these two subsections of section 889(f)(3), Congress in the Secure Networks Act has identified as "covered" equipment both "telecommunications equipment" and "video surveillance equipment" produced by these entities or used in the provision of video surveillance or telecommunications services; prior to inclusion of section 889(f)(3) in Secure Networks Act section 2(c)(3), this equipment was subject only to the executive branch's prohibitions of procurement under section 889 of the earlier enacted NDAA because such equipment can pose an unacceptable risk to national security. To remove "telecommunications equipment" and "video surveillance equipment" produced by Hytera, Hikvision, and Dahua from the Covered List, as their representatives request, would ignore Congressional intent regarding its recognition and determination that use of such equipment can pose an unacceptable risk to national security. In our view, Congress identified this equipment as posing an unacceptable risk, and we are not in position to question that or not include it on the Covered List..[414] Furthermore, Congress passed the Secure Equipment Act in response to the instant Commission proceeding and the then-current Covered List, and Congress expressly mandated that the Commission prohibit authorization of equipment on the Covered List as it had proposed to do in the *NPRM* in this proceeding. Congress therefore intended the prohibition that the Secure Equipment Act requires us to adopt to include the telecommunications equipment and the video surveillance equipment that already was on the Covered List. Given our conclusion here that the arguments of Hytera, Hikvision, and Dahua representative fail on the merits, we need not address Motorola's contention that their arguments must be denied on the basis of the Hobbs Act.[415]

169. We disagree with the assertions that telecommunications and video surveillance equipment produced by Hytera, Hikvision, and Dahua are not "covered" because their respective equipment does not meet the "capability" requirements under section 2(b) of the Secure Networks Act either with respect to being capable of routing or redirecting user data traffic or permitting visibility into any user data or packets or causing the network to be disrupted remotely. As discussed above, the Commission already has concluded in both the *Supply Chain 2nd R&O* and the *Supply Chain 3rd R&O* that the Commission need not make any Secure Networks Act § 2(b)(2) "capability" assessment regarding Hytera, Hikvision, or Dahua equipment, under either § 2(b)(2)(A) or (B) of the Secure Networks Act, since, in effect, Congress under § 889(f)(3) of the 2019 NDAA has made that capability determination pursuant to § 2(b)(2)(C),[416] concluding that video surveillance and telecommunications equipment produced by these entities is "covered" equipment insofar as Congress has determined that it is capable of "otherwise posing an unacceptable risk" to national security. This decision is further supported by the Commission's discussion of a section 2(b)(2)(C) determination in the *Supply Chain 2nd R&O*. It noted that if an enumerated source it its determination indicates that a specific piece of equipment or service poses an unacceptable risk to the national security of the United States and the security and safety of United States persons, the Commission need not conduct an analysis of the capabilities of the equipment and instead will automatically include this determination on the Covered List.[417] Congress, the enumerated source with regard to determinations about this equipment, has already performed the analysis on whether the equipment – such as video surveillance equipment specifically identified under section 889(f)(3)(B) and (C) – poses an unacceptable risk to the national security of the United States or

[413] 2019 NDAA § 889(f)(3)(A)-(C).

[414] As the Commission has underscored repeatedly, the Commission has no discretion to disregard determinations by any of the four enumerated sources. *See Supply Chain 2nd R&O*, 35 FCC Rcd at 14312, para. 60 (citing the Secure Networks Act § 2(c)).

[415] As noted above, that no representatives of Hytera, Hikvision, or Dahua challenged inclusion of such equipment on the Covered List when that list was initially published on March 12, 2021.

[416] *Supply Chain 2nd R&O*, 35 FCC Rcd at 14315-16, para. 67.

[417] *Id.* at 14320-21, paras. 80-81; *see id.* at 14322, para. 85.

the security and safety of United States persons as part of its determination. For these reasons as well, we also disagree with PowerTrunk insofar as it opposes our adoption of a prohibition on future authorizations of any "covered" equipment that it produces. Regardless of whether PowerTrunk may have been permitted in 2018 for use by certain public safety entities, the issue before us in this proceeding is whether to permit future authorizations of PowerTrunk telecommunications and video surveillance equipment. We reject the argument that any such PowerTrunk equipment should be exempted from the prohibition that the Commission proposed in the *NPRM*, based on a determination made pursuant to the Secure Networks Act, and that Congress in the Secure Equipment Act directed the Commission to adopt.

170. In addition, we reject the arguments that video surveillance equipment is not "covered" under the Secure Networks Act because it is not "communications equipment" or "essential to the provision of advanced communications service," as defined in sections 9(4) of the Act. As discussed above, in its *Supply Chain 2nd R&O*, the Commission has already interpreted "communications equipment or service" and what is "essential," codifying that interpretation in section 1.50001(c) of the Commission's rules: "The term 'communications equipment or service' means any equipment or service used in fixed and mobile networks that provides advanced communications service, provided the equipment or service includes or uses electronic components."[418] We also reject Hikvision USA's further contention that video surveillance equipment is not "used in" fixed and mobile networks, and Hikvision's and Dahua's assertions that such equipment is only "peripheral" equipment and not network equipment and hence not "covered." In identifying such equipment as covered communications equipment under the Secure Networks Act, by reference to section 889(f)(3), Congress intended to capture such video surveillance equipment as "covered" equipment, even if is not core network equipment since the equipment is used (and indeed required) in the provision of a certain type of advanced communications service, i.e., video surveillance services. In addition, we are not persuaded by arguments that because the video surveillance and telecommunications equipment produced by the entities does not have to be interconnected to a telecommunications or broadband network, it is not "covered" equipment. As acknowledged, Hikvision, Dahua, and Hytera equipment can be interconnected, and often is. We also note that some of the video surveillance equipment is part of a cloud-based system requiring interconnection.

171. In sum, "covered" equipment on the Commission's Covered List includes "telecommunications equipment" as well as "video surveillance equipment" produced by Hytera, Hikvision, and Dahua (and their subsidiaries or affiliates), and was properly placed on the Covered List first published by PSHSB in March 2021. The Commission's existing rules rightfully prohibit the use of federal support to purchase or obtain any "covered" equipment on the Covered List, which appropriately includes a prohibition concerning this video surveillance and telecommunications equipment. We also note that our actions are consistent with the efforts of the Executive Branch, discussed above, in identifying and implementing a prohibition on procurement with respect to certain "covered" video surveillance and telecommunications equipment produced by Hytera, Hikvision, and Dahua.

(b) Prohibition concerning equipment authorization of "video surveillance and telecommunications equipment" "[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes"

172. *Background.* As discussed above, Hytera, Hikvision, and Dahua representatives each contend that section 889(f)(3)(B) of the 2019 NDAA precludes the Commission from adopting a blanket prohibition on their video surveillance and telecommunications equipment, asserting that provision only prohibits use of such equipment for certain specified types of uses/users, but not others. Several commenters, many representing business dealers that sell Hytera, Hikvision, and Dahua products,

[418] *Id.* at 14309, para. 52 and 14310-11, paras. 55-56; 47 CFR § 1.50001 Definitions, § 1.50001(c).

including video surveillance products, to a variety of users (e.g., businesses, manufacturers, schools, residences, and public safety entities) claim that the equipment is safe and reliable, and oppose prohibiting authorization of that equipment.[419] IPVM, JVCKenwood, Motorola, and Noah Venafric, however, support such a prohibition.[420]

173. Hytera, Hikvision, and Dahua representatives contend that the very language of section 889(f)(3)(B) of the 2019 NDAA establishes that what is "covered" equipment is limited in scope, and includes their telecommunications and video surveillance equipment only "to the extent it is used for public safety and security," citing the specific language used in the Covered List.[421] In their views, the language of this provision prevents the Commission from adopting a categorical or blanket prohibition on equipment authorization of their video surveillance equipment, given that much of that equipment is not (or would not be) actually used by public safety, critical infrastructure, or other national security purposes.[422] As further support of this view, Hikvision and Hytera point to "decision tree" guidance provided by GSA regarding the 2019 NDAA § 889 prohibition on federal agencies' procurement or use of "covered" equipment under § 889(f)(3)(B); they assert that this guidance indicates that §889(f)(3)(B) only prohibits procurement of video surveillance and telecommunications equipment produced by Hikvision, Dahua, or Hytera that is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, or other national security purposes, and does not otherwise prohibit use of such equipment.[423] They contend that the Commission cannot expand the scope of "covered" equipment beyond what is included on the Covered List.[424] Hytera US specifically requests that the Commission provide clear guidance that the "covered" equipment on the Covered List only concerns a prohibition on those specified uses.[425] Finally, many companies, representing different

[419] Several commenters discussed their opposition to a ban on Hytera equipment. *See, e.g.*, Alpha Prime Communications Comments at 1 (Hytera equipment is sold to small businesses, small manufacturers, and schools); Eagle Communications Comments at 1 (sells two-way radio solutions to businesses); FreCom Inc. Comments at 1 (servicing dealer for radio products for schools and extended living facilities); RadioMax Communications Inc. at 1 (Two-way radio communication company that serves first responders, public safety companies, school districts, and other businesses). Others commented on their opposition to a ban on Hikvision and Dahua equipment. *See, e.g.*, Chown Hardware at 1 (has multimillion projects with several local properties); Eastern CCTV Comments at 1 (sells Dahua equipment to system integrators and system installers who work on small to medium-sized businesses and residential projects).

[420] IPVM Comments at 1 (Hikvision and Dahua equipment is a danger to national security); JVCKenwood Comments at 2 (Commission should, and it is in fact obligated, pursuant to extant legislation and outstanding executive orders, to prohibit the authorization of equipment manufactured by covered entities); Motorola Reply Comments at 9 (Commission should reject requests made by manufacturers whose equipment is on the Covered List (the Covered Entities) that the Commission should carve out their equipment from the Covered List); Venafric Reply Comments at 1 (comments and outside literature provide more than sufficient evidence that equipment from Huawei, ZTE Corporation, Hytera, Hangzhou Hikvision, and Dahua pose an unacceptable threat to national security).

[421] *See, e.g.*, Hytera US Comments at 10; Dahua USA Comments at i, 15-16; Dahua USA Reply at 15; Hikvision USA Reply at ii, 19-20.

[422] *See, e.g.*, Hytera US Comments at ii, 10; Hytera Ltd Reply Comments at 2; Hikvision USA Comments at 5-6, 33-37 (section 889(f)(3) only restricts funding or use of Hikvision equipment for certain purposes, leaving the vast majority of Hikvision products and end users unaffected); Hikvision Reply at ii, 19-25; Hikvision USA Nov. 22 *Ex Parte* at 2-3; Dahua USA Comments at i, 17; Dahua USA Reply at 13; Dahua USA Dec. 10 *Ex Parte* at 2.

[423] Hikvision USA Comments at 36 & n.80 (citing GSA's August 13,2020 "SCRM Criteria for Section 889 Part B, at 1); Hytera US Reply at 2-3 (same). *See* https://www.gsa.gov/node/137296.

[424] Hikvision USA Nov. 22, 2012 *Ex Parte* at 2; Dahua USA Dec. 10, 2022 *Ex Parte* at 1; Hytera US Reply Comments at 3; Hytera Ltd. Reply Comments at 1-2.

[425] *See, e.g.*, Hytera US Comments at 7, 10.

business dealers that sell equipment produced by Hytera, Hikvision, or Dahua, also filed comments opposing prohibitions on authorizing of equipment produced by the latter companies.[426]

174. Motorola disagrees with arguments that § 889(f)(3)(B) of the 2019 NDAA requires that equipment is "covered" only if it is actually "used" in a fixed or mobile broadband network to be included on the Covered List. First, Motorola notes that the statutory language itself does not include the term "used," and in Motorola's view restricting "covered" equipment in such a way is contrary to the language in section 889(f)(3)(B)."[427] In keeping with its view that the Commission should interpret what is "covered" broadly for purposes of the equipment authorization program, Motorola contends that no need exists for Hytera, Hikvision, and Dahua's equipment to be "used" exclusively by public safety for such equipment to be on the Covered List. Given that section 889 of the 2019 NDAA provides that covered telecommunications or services includes "[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera, Hikvision, or Dahua (and their subsidiaries and affiliates)," Motorola contends that any equipment "offered to public safety customers" would satisfy this standard," regardless of whether the equipment may be offered to or used by non-public safety customers as well.[428] In addition, Motorola asks that the Commission clarify the language in the Covered List on this issue by eliminating the "to the extent used for" language, stating that the Commission has a statutory obligation to do so. Motorola also asks that the Commission further clarify that the types of equipment that fall within the Covered List categories include video surveillance and telecommunications equipment produced by Hytera, Hikvision, and Dahua and that "covered" equipment need only be "for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes."[429]

175. NTCA also points to the language in the Commission's Covered List that provides that "covered" equipment includes video surveillance equipment produced by Hytera, Hikvision, and Dahua "to the extent that it is used for" certain public safety, critical infrastructure, and national security purposes, and notes that the same equipment is used by individuals and private businesses. NCTA asks that the Commission clarify how it will apply the equipment authorization process to equipment that is "covered" for certain uses while not "covered" for other uses.[430]

176. *Discussion*. In adopting the prohibition on authorizing "covered" equipment, we are guided by the specific determination set forth in section 889(f)(3)(B) of the 2019 NDAA regarding "covered" "telecommunications equipment" and "video surveillance equipment" produced by Hytera, Hikvision, or Dahua (or their subsidiaries and affiliates). In the *NPRM*, the Commission proposed to prohibit authorizing any "covered" equipment on the Covered List.[431] As discussed in the *NPRM* and above, pursuant to the Secure Networks Act section 2(c), the Commission must rely solely on the

[426] *See, e.g.*, Chown Hardware Comments at 1; Eastern Security Comments at 1.

[427] Motorola May 3, 2022 *Ex Parte* at 7.

[428] Motorola Mar. 24, 2022 *Ex Parte* at 5; Motorola May 3, 2022 *Ex Parte* at 7.

[429] Motorola Mar. 24, 2022 *Ex Parte* at 6; Motorola May 3, 2022 *Ex Parte* at 7-8. Motorola also asks that the Commission, in its rules requiring applicant attestations in the equipment authorization process, require that applicants certify that the equipment for which authorization is sought "will not be marketed, sold, offered, or otherwise made available, either directly or indirectly, to public safety, government security, critical infrastructure, and other national security customers." Motorola May 27, 2022 *Ex Parte* at 1-2.

[430] NTCA Comments at 5.

[431] *NPRM*, 36 FCC Rcd at 10596, para. 38. *See also id.* at 10595-96, para. 37 (quoting the March 2021 Covered List, which included, as covered equipment, video surveillance and telecommunications equipment produced by Hytera, Hikvision, and Dahua "to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes").

determinations made by the four enumerated sources identified in that section.[432] Section 889(f)(3)(B) by its terms provides that "covered" equipment includes "video surveillance and telecommunications equipment" produced by Hytera, Hikvision, and Dahua "[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes."[433] Accordingly, the Commission cannot and will not approve of any application for equipment authorization that would allow the marketing and selling of such equipment for those specified uses. At the same time, this determination only includes, as "covered" equipment, video surveillance and telecommunications equipment produced by these entities that is for those particular purposes. Thus, at this time, in the absence of any other of the three identified and specific determinations made by any of the Executive Branch agencies identified in section 2(c) of the Secure Networks Act, the Commission cannot expand "covered" beyond that determination by adopting a blanket or categorical prohibition on authorizing equipment produced by these entities for those other purposes. Our approach regarding this equipment is consistent with the Commission's previous interpretations of section 889(f)(3)(B) in the 2020 *Supply Chain 2nd R&O* and in the language specified in the Covered List, in which the Commission stated that this equipment produced by Hytera, Hikvision, and Dahua (and their subsidiaries and affiliates) is "covered" "to the extent used" for these specified purposes.[434] And, as discussed above, federal agencies in implementing the federal agency procurement prohibitions under section 889 have interpretated this statutory language regarding the scope of "covered" equipment in a like manner.[435]

177. Accordingly, we are prohibiting authorization to market and sell Hytera, Hikvision, and Dahua "telecommunications equipment" and "video surveillance equipment" (and that produced by their subsidiaries and affiliates) "[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes." For any equipment authorization application for video surveillance and telecommunications equipment produced by these entities, we will impose strict and appropriate conditions on any approved grant, consistent with the Commission's equipment authorization rules.[436] Specifically, the Commission will only conditionally authorize the marketing and sale of such equipment authorization subject to this prohibition. The Commissions also will require labeling requirements that prominently state this prohibition. As a condition of the equipment authorization, the Commission also will also impose stringent marketing and sale prohibitions associated with the equipment, which will apply not only with respect to these entities (and their subsidiaries and affiliates), but also to their equipment distributors, dealers, or re-sellers, i.e., every entity down the supply chain that markets or offers the equipment for sale or that markets or sells the equipment to end-users.

178. Based on the record before us, we also are concerned that adopting conditions alone will not be sufficient to ensure that "covered" equipment is not over time marketed, or ultimately sold, for the purposes prohibited under section 889(f)(3)(B) of the 2019 NDAA. Given that "covered" equipment poses an unacceptable risk if used "[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes," we adopt additional restrictions as described herein to prevent marketing and sale of Hytera, Hikvision, or Dahua "telecommunications equipment" or "video surveillance equipment" for use for the purpose of public safety, government security, critical infrastructure, or national security.

---

[432] *NPRM*, 36 FCC Rcd at 10595-96, para. 37 (equipment on the Covered List is based exclusively on determinations made by Congress and by other Government agencies); Secure Networks Act, section 2(c).

[433] Section 889(f)(3)(B) of the 2019 NDAA.

[434] *Supply Chain 2nd R&O*, 35 FCC Rcd at 14316, para. 68.

[435] See paragraph 13, *supra*; *see* https://www.acquisition.gov/FAR-Case-2019-009/889_Part_B.

[436] The Commission's rules authorize adoption of various conditions on equipment authorizations. *See* 47 CFR §§ 2.915 (grant must be in public interest); 2.295(a), (d) (labeling requirements on statements); 2.297(c) (restrictions on marketing, advertising, brochures, etc.); 2.935 (electronic labeling).

179. Hytera, Hikvision, and Dahua representatives generally contend that their equipment is not marketed or promoted for these prohibited purposes. Hytera US, for instance, states that it does not market its equipment, including its P25 and FirstNet compatible equipment, to public safety entities.[437] Hikvision USA states that its dealers are responsible for selling its equipment, that it does not sell any of its products directly, either to consumers or to the U.S. government, and that does not collect end-users data.[438] Hikvision USA further states that it does not have a systematic way to know the identity of end users, and that it is "confident" that government entities, critical infrastructure (e.g., power, water, and other utilities) are only a *de minimus* portion of Hikvision's U.S. sales, with the vast majority of its cameras not used by public safety, security of government facilities, or critical infrastructure.[439] In its submissions, Dahua USA states that it has approximately 20 authorized distributors and more than 5,000 dealers (e.g., system integrators, installers, and other resellers) in the United States, and that it currently has "no control" over any dealer's final decision regarding purchasing of the Dahua equipment for a particular project or customer.[440] It further asserts that it does not specifically market or target government facilities, critical infrastructure sectors, or customers that provide national security, and contends that, while it is possible that some Dahua products have been purchased by state or local governments, such uses are only *de minimus* in relation to the overall base of its products.[441] Motorola, in turn, points to a Hytera website devoted to equipment for public safety use, including for police and fire service, and also notes Hytera's worldwide marketing and sales of equipment for public safety.[442] While Hytera Ltd contends that the activities the Motorola references only concern Hytera activities outside of the United States,[443] Motorola responds that Hytera's Facebook page promotes offerings that are important to public safety, and Hytera US's website that state that since Hytera's founding in 1993 it has been a leading provider of wireless solutions for public safety.[444] Motorola also provides evidence that dealers of Hytera equipment have expressly indicated that their clients and customers include purchasers of Hytera communications systems and mobile radios by local, state, and federal agencies, police, sheriff and other law enforcement groups, fire and emergency first responders, and hospitals.[445] IPVM's attention focuses on Hikvision and Dahua video surveillance equipment, contending that Hikvision and Dahua each widely markets its video surveillance equipment to U.S. companies while also indicating that their respective equipment video surveillance equipment does not belong on the Covered List.[446] The Center for Security and Emerging Technology also submitted its recent report examining government approaches to foreign technology threats, in which it found that between 2015 and 2021 nearly 1,700 state and local governments had purchased equipment on the Covered List, including equipment produced by Hytera, Hikvision, and Dahua.[447] We note that in more recent submissions, Dahua USA proposes that it will adopt product and package labeling that would include clear statements that Dahua equipment cannot be used for any of the purposes identified in section 889(f)(3)(B), and states that it plans to implement

[437] Hytera Ltd, PowerTrunk, and Hytera US June 3, 2022 *Ex Parte* at 1.

[438] Hikvision USA Comments at 16.

[439] Hikvision USA Aug. 29, 2022 *Ex Parte* at 3-4.

[440] Dahua USA June 28, 2022 *Ex Parte* at 1-2.

[441] *Id.* at 3-4.

[442] Motorola June 17, 2022 *Ex Parte* at 1-2.

[443] Hytera Ltd June 30, 2022 *Ex Parte* at 1-2.

[444] Motorola Aug. 10, 2022 *Ex Parte* at 1-2.

[445] *Id.* at 2-3 (citing court filings by certain dealers of Hytera equipment).

[446] IVPM Jan. 11, 2022 *Ex Parte* at 1-3.

[447] *See* Jack Corrigan Comments & attached report by the Center for Security and Emerging Technology, "Banned in D.C.[:] Examining Government Approaches to Foreign Technology Threats," at 18-24.

record-keeping measures to help keep track of sales of "covered" equipment and ensure transparency throughout the flow of distributions and sale to end-users.[448]

180. Based on this record, which highlights the lack of oversight that Hytera, Hikvision, and Dahua have over the marketing, distribution, and sales of their respective equipment in the United States, we are not confident that, absent additional prescriptive measures and Commission oversight, Hytera, Hikvision, and Dahua "telecommunications equipment" or "video surveillance equipment" will not be marketed and sold for those purposes that are prohibited under section 889(f)(3)(B) of the 2019 NDAA. Accordingly, we will require that, before the Commission will permit an equipment authorization of any "telecommunications equipment" or "video surveillance equipment" produced by Hytera, Hikvision, or Dahua (or their subsidiaries or affiliates), these entities must each seek and obtain Commission approval for its respective plan that will ensure that such equipment will not be marketed or sold "[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes." Any such plan must demonstrate that effective measures are in place that will ensure that equipment distributors, equipment dealers, or others in the supply and distribution chains associated with marketing or sale of such equipment are aware of this restriction and do not market or sell such equipment to entities for the purposes mentioned above. Such a plan must include well-articulated and appropriate measures at the distributor and dealer levels to ensure that the entity does not market or sell for prohibited purposes. Before any Hytera, Hikvision, or Dahua "telecommunication equipment" or "video surveillance equipment" will be authorized for market or sale, the applicant seeking approval of any "covered" equipment produced by any of these entities (or their subsidiaries or affiliates) must submit a specific plan associated with the equipment, which will be reviewed by the full Commission and only approved if the measures that are and will be taken are sufficient to prevent the marketing and sale of such equipment for purposes prohibited under section 889(f)(3)(B) of the 2019 NDAA.

181. In section III.C.5, below, we provide guidance on what constitutes "telecommunications equipment" and "video surveillance equipment," as well as clarify the scope of the prohibition under section 889(f)(3)(B) concerning "[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes." Finally, we note that the Commission's actions in this Report and Order, including this particular prohibition on authorization of "telecommunications equipment" and "video surveillance equipment" produced by Hytera, Hikvision, and Dahua, are among the several Commission and whole-of-government approaches underway and that are continuing to evolve. As discussed below, as future determinations are made under section 2(c) of the Secure Networks Act regarding "covered" equipment that poses an unacceptable risk to national security, and the Covered List is updated accordingly, authorizations of such equipment will be prohibited as well.

3. "Covered" equipment produced by subsidiaries and affiliates

182. As discussed above, on the current Covered List, "covered" equipment produced by "subsidiaries and affiliates" of the companies named on the Covered List also are included within the scope of "covered" equipment, and authorization of such equipment will be prohibited as "covered" equipment as a result of our revisions to the equipment authorization program rules adopted in this proceeding. Applicants seeking equipment authorizations will be required to attest (in the form of a written and signed certification) that the equipment for which they are seeking authorizations is not "covered" equipment produced by any of the entities identified on the Covered List, which thus could include equipment produced by the named entities on the Covered List or produced or by any subsidiaries or affiliates of those entities.[449]

---

[448] Dahua USA Sept. 22, 2022 *Ex Parte* at 2.

[449] Section III.C.2. By entities named on the Covered List, we mean the specific entity actually named on the Covered List. As we have noted, the current Covered List specifically names five entities as producing "covered"

(continued….)

183. *Definitions.* We address here the relevant definitions that the Commission will apply in our rules implementing the prohibition on authorization of "covered" equipment to the extent such equipment includes equipment produced by subsidiaries and affiliates of entities specifically named on the Covered List.[450] We start with "affiliate," for which we adopt the a definition consistent with that adopted by the Commission in its *Supply Chain 2nd R&O.* That order defined "affiliate" as "a person that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another person," referencing the definition of "affiliate" contained in section 3 of the Communications Act (47 U.S.C § 153(2)).[451] We note that the definition of affiliate in the Communications Act further states that "[f]or purposes of this paragraph, the term 'own' means to own an equity interest (or the equivalent thereof) of more than 10 percent,"[452] and we adopt such further clarification here. For purposes of implementation in our equipment authorization program, we define "affiliate" as an entity that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another entity, where the term "own" means to have, possess, or otherwise control an equity interest (or the equivalent thereof) of more than 10 percent.

184. As for "subsidiary," we note generally that a subsidiary is an affiliate that is directly or indirectly controlled by an entity (e.g., corporation) with at least a greater than 50% share.[453] In the context of reviewing foreign ownership under section 310(b) of the Communications Act,[454] the Commission's rule defines a "subsidiary" of a licensee as "any entity in which a licensee owns or controls, directly and/or indirectly, more than 50 percent of the total voting power of the outstanding voting stock of the entity, where no other individual or entity has de facto control."[455] We believe that adopting a broader definition of subsidiary than the one set forth in our foreign ownership rules is appropriate here in light of the national security purposes of the Secure Equipment Act. We believe that adopting a broader definition of subsidiary than the one set forth in our foreign ownership rules is appropriate here in light of the national security purposes of the Secure Equipment Act. For purposes of implementing the prohibition on "covered" equipment, we define "subsidiary" of an entity named on the Covered List as any entity in which such named entity directly or indirectly (1) holds *de facto* control or (2) owns or controls more than 50% of the total voting power of the entity's outstanding voting stock..

185. *Names of entities identified on the Covered List that produce "covered" equipment, including subsidiaries and affiliates.* We also are adopting a requirement that, to the extent the Covered List identifies named entities as well as certain unnamed associated entities – such as subsidiaries or affiliates – as producing "covered" equipment, each such entity specifically named on the Covered List as producing "covered" equipment must submit information to the Commission regarding that named entity's associated entities. As discussed above, the current Covered List identifies equipment produced

---

equipment. Among these, for instance, it specifically names "Huawei Technologies Company." *See September 2022 Covered List Public Notice*, Appendix. The Covered List also makes clear that "covered" equipment includes equipment produced by each named entity's subsidiaries and affiliates (which are not specifically named). *Id.*

[450] No commenting parties commented on the appropriate definition for either "subsidiary" or "affiliate" for purposes of this proceeding.

[451] *Supply Chain 2nd R&O*, 35 FCC Rcd at 14333, para. 113; *see also* Secure Networks Act § 9(6)(B); 47 U.S.C. § 153(2). The Commission also applied this definition in its *Supply Chain 3rd R&O*, 36 FCC Rcd at 11963-64, para. 15.

[452] 47 U.S.C. § 153(2).

[453] The Securities and Exchange Commission defines a subsidiary as follows: "[a] subsidiary of a specified person is an affiliate controlled by such person directly, or indirectly through one or more intermediaries." 17 CFR § 210.1–02(x).

[454] 47 U.S.C. § 310(b).

[455] 47 CFR § 1.5000(d)(10); *see also* 47 CFR § 1.5000(d)(11).

by certain named entities and their subsidiaries and affiliates as "covered" equipment.[456] As Motorola notes, the entities on the Covered List do not currently publicly disclose detailed information about their corporate relationships, including the names of their subsidiaries and affiliates, and it contends that it is "imperative" that the Commission have visibility into these relationships.[457] In implementing rules and procedures to prohibit authorization of such "covered" equipment produced by particular entities named on the Covered List and their associated entities (e.g., their respective subsidiaries and affiliates), we find that it is critical that the Commission, as well as applicants for equipment authorizations, TCBs, and other interested parties, have the requisite, transparent, and readily available information of the particular entities that in fact are such associated entities of the named entities on the Covered List.[458] We find that having this information on the names of such associated entities promotes effective implementation of and compliance with the prohibition, by providing the Commission and TCBs in advance of reviewing any equipment authorization applications with a list of all those entities to which the Covered List applies. Requiring that this information be provided to the Commission and made public aligns with the regulatory requirements that the Commission proposed in the *NPRM* and that we are adopting, namely placing responsibilities on applicants to attest that their equipment is not "covered" equipment produced by any of entities identified on the Covered List. This also adds another important informational element to the overall comprehensive regulatory scheme and approach that we are taking to ensure that applications for authorization of "covered" equipment are not submitted to the Commission and that no such equipment authorization is granted. Requiring this information is both reasonable and justified in keeping with our goal of effectively ensuring that "covered" equipment determined as posing an unacceptable risk to national security under the Secure Networks Act, and prohibited from authorization under the Secure Equipment Act, is not authorized, and helps to ensure that the Commission meet the mandate in the Secure Equipment Act that the Commission not approve grant of any "covered" equipment.[459] Finally, it is also critical that such information be up-to-date and maintained in a place for all interested parties to reference for purposes of compliance with our rules, including the applicants' attestation requirements.

186. Accordingly, if "covered" equipment on the Covered List includes equipment produced by named entities as well as associated unnamed entities (e.g., their subsidiaries and affiliates), we will require that each entity specifically named on the Covered List that produces "covered" equipment submit a complete and accurate list to the Commission, within 30 days of effective date of the rules, identifying the names of such associated entities that produce equipment that requires an equipment authorization under the rules we are adopting in this Report and Order, and must provide up-to-date information on any

[456] We think it likely that, under any updated Covered List that identifies "covered" equipment produced by entities other than those named entities, such list will also include, within the ambit of "covered" equipment, "covered" equipment produced by subsidiaries and affiliates of named entities. Nonetheless, the possibility exists that a future Covered List could identify other types of entities associated with the named entities that produce "covered" equipment. If so, then under the requirements that we are adopting here, the named entity would be required to submit information on such associated entities.

[457] *See* Motorola Mar. 24, 2022 *Ex Parte* at 5-6 (supporting a requirement that each applicant certify that it is not affiliated with or a subsidiary of a company with equipment on the Covered List).

[458] As discussed in Section III.B.2.a, above, we also are adopting a requirement that applicants for equipment certification indicate whether they are any entities identified on the Covered List as producing "covered" equipment.

[459] We note that the Commission may require information that is otherwise kept confidential to be submitted to it and may publicly reveal that information when, on balance, it is in the public interest to do so. 47 U.S.C. § 154(j); *FCC v. Schreiber*, 381 U.S. 279, 291-92 (1965); *Applications of Charter Communications, Inc., Time Warner Cable Inc., and Advance/Newhouse Partnership for Consent to Assign or Transfer Control of Licenses and Authorizations*, Order, 30 FCC Rcd 10360,10365-67, paras. 13, 15 (2015); *Examination of Current Policy Concerning the Treatment of Confidential Information Submitted to the Commission*, GC Docket No. 96-55, Notice of Inquiry and Notice of Proposed Rulemaking, 11 FCC Rcd 12406, 12414-15, para. 15 (1996). Balancing the various interests, we find that the public interest in the public knowing which entities are subsidiaries or affiliates of entities on the Covered List outweighs whatever private interest those entities may have in keeping this information confidential.

changes to the list with respect to any such entities. For each such associated entity (e.g., subsidiary or affiliate), the entity named on the Covered List must provide the following information: full name, mailing address and physical address (if different from the mailing address), email address, and telephone number. If there are changes to a named entity's list of such associated entities, that entity must submit such updated information to the Commission within 30 days of the change(s), and indicate the date on which the particular change(s) occurred. These submissions must be supported by an affidavit or declaration under penalty of perjury, signed and dated by an authorized officer of the named entity on the Covered List with personal knowledge verifying the truth and accuracy of the information provided about the entity's associated entities. The affidavit or declaration must comply with section 1.16 of the Commission's rules.[460] This information on these entities will be posted on the Commission's website as an Appendix to the guidance on "covered" equipment posted by OET and PSHSB, and will be updated with any updated information that the Commission receives. Applicants requesting equipment authorizations will be able to reference this information when making attestations regarding the producer of equipment for which they seek authorizations, as will TCBs, the Commission, and other interested parties.[461]

4. Re-branded ("white label") equipment

187. Particular equipment, including products approved through the Commission's equipment authorization program, may be produced by particular companies or manufacturers and subsequently re-branded by other companies. We note, for instance, that Dahua USA acknowledges that its video surveillance equipment may be re-branded and sold under re-branded names.[462] IPVM also notes that Hikvision and Dahua video cameras often have been relabeled and sold under another name.[463]

188. As discussed above, we are prohibiting authorizing "covered" equipment "produced" by any of the named entities (as well as their subsidiaries or affiliates) on the Covered List. Under the prohibition on authorizing equipment "produced" by entities on the Covered List we also are precluding any equipment application by any other entity to the extent that the equipment for which authorization is sought had been produced by entities identified on the Covered List but has been re-branded or re-labeled with other names or associated with other companies. Re-branding of equipment does not change the status of whether the equipment itself is "covered" equipment prohibited from equipment authorization.

5. Guidance on implementing the prohibition on authorizing "covered" equipment in the Equipment Authorization Program

189. As discussed above, we affirm the Commission's earlier decisions and conclude that, pursuant to the Secure Networks Act and section 889(f)(3) of the 2019 NDAA, "covered" equipment on the current Covered List includes both "telecommunications equipment" and "video surveillance equipment" produced by Huawei and ZTE (and their subsidiaries and affiliates), as well as such equipment produced by Hytera, Hikvision, and Dahua (and their subsidiaries and affiliates) to the extent used "[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes." Under the rules that we adopt today, the Commission will no longer permit the authorization to market or sell any such "covered" equipment in our equipment authorization program. As an integral part of our implementation of this prohibition, under our revised part 2 equipment authorization rules we will require each applicant for equipment authorization to provide in its application an attestation (in the form of a written and signed certification) that the equipment in its application is not "covered" equipment. Below we provide additional clarity on

[460] 47 CFR § 1.16.

[461] While applicants and other interested parties can reference this information for purposes of their attestations, we note that applicants' attestations must be based on conducting their own due diligence to ensure compliance with our rules.

[462] Dahua USA Comments at 2; Dahua USA Reply Comments at 2-3.

[463] IPVM Jan. 11, 2022 *Ex Parte* at 3-4.

what constitutes "covered" equipment that will be prohibited, as several have requested.[464] As a general matter, given the importance of preventing "covered" equipment from being made available for uses that would pose an unacceptable risk to national security or the security of U.S. persons, the terms of determinations made by any of the four enumerated sources and incorporated into the Covered List should be interpreted broadly.

190. In proposing in the *NPRM* to require applicants for equipment certification to attest that the subject equipment is "not" covered, the Commission recognized the importance of providing guidance to applicants, TCBs, and other interested parties.[465] In particular, the Commission proposed to direct Commission staff (OET, working with PSHSB, WCB, IB, and EB) to develop pre-approval guidance or other guidance to assist in implementing the Commission's prohibition on authorization of "covered" equipment.[466] Here we provide guidance to Commission staff as well as applicants, TCBs, and other interested parties regarding the administration and implementation of the prohibition of the authorization of "covered" equipment through the attestation process, the TCBs' assessment, and the Commission in its implementation and monitoring of the equipment authorization process to ensure that "covered" equipment is not authorized for marketing or sale.

191. For purposes of the implementation of the equipment authorization program, we interpret the terms "telecommunications equipment" and "video surveillance equipment" broadly to ensure that equipment that could pose an unacceptable risk is not authorized, in keeping with our proposal and its acknowledgement in the Secure Equipment Act of 2021. As discussed below, we delegate to OET and PSHSB, working with other bureaus/offices as appropriate, the authority to provide additional clarity with regard to the scope of covered equipment for purposes of our equipment authorization program, to make such information on the Commission's website, and to revise that information as appropriate. We underscore the importance for each applicant seeking authorization of equipment to exercise due diligence in preparing and submitting its attestation that the subject equipment for which it seeks authorization for market or sale is not "covered." At the time of the filing of its application for certification of equipment, each applicant must have reviewed the Commission rules and guidance set forth on its webpage, and have determined through due diligence that the subject equipment in its application for certification is not "covered." As discussed above, false statements or representations that the subject equipment is "not" covered will result in denial of an application or revocation of the equipment authorization and potentially additional enforcement action.[467]

192. As noted in the *NPRM*, the Commission authorizes a wide array of equipment. Under existing rules for certification, such equipment includes base stations, transmitters associated with various licensed services (including mobile phones, land mobile radios), Wi-Fi access points and routers, home cable set-top boxes with Wi-Fi, laptops, intelligent home devices, and various wireless consumer equipment.[468] Equipment that is subject to authorization under existing SDoC procedures includes certain microwave and broadcast transmitters, certain private land mobile equipment, certain equipment for

[464] *See, e.g.*, Hytera US Comments at 4, 6, 9; CTIA Comments at 11, 16-17 (requirement for attestation must be accompanied by clarity in the form of Commission guidance about the definitions of "telecommunications equipment" and "video surveillance equipment," as well as whether handsets are "covered"); NTCA Comments at 4-5; Motorola March 24, 2022 *Ex Parte* at 5-6 (absent greater clarity regarding categories of "covered" equipment, applicants attesting that their equipment is not "covered" may abuse the prohibition on authorizing "covered" equipment).

[465] *NPRM*, 36 FCC Rcd at 10600-01, para. 49.

[466] *Id.*

[467] *See* Section III.B.6.a.

[468] *NPRM*, 36 FCC Rcd at 10592, 10598-99, paras. 28, 44.

unlicensed use (e.g., business routers, internet routers, firewalls, internet appliances, surveillance cameras, business servers, and certain ISM equipment).[469]

193. In addition to providing guidance clarifying the nature of "telecommunications equipment" and "video surveillance equipment," we also discuss below the scope of our prohibition with regard to authorization of Hytera, Hikvision, and Dahua "telecommunications equipment" and "video surveillance equipment." Pursuant to the determination made by Congress under section 889(f)(3)(B), and as identified on the Covered List, such equipment produced by these entities is "covered" "for purposes of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes."

194. *Telecommunications equipment.* Considering the importance of prohibiting authorization of "covered" equipment that poses an unacceptable risk to national security, we interpret "telecommunications equipment" broadly for purposes of the Commission's equipment authorization program. This approach is consistent with our earlier decisions that broadly define "communications equipment" under the Secure Networks Act.[470] It also accords with congressional intent in the Secure Equipment Act of 2021.

195. In particular, we interpret "telecommunications equipment" as broadly as we previously defined "communications equipment." Under the approach adopted here, "telecommunications equipment" means any equipment used in fixed or mobile networks that provides advanced communications service, provided the equipment includes or uses electronic components, as defined under section 1.50001(c).[471] Further, taking into consideration the definition of "advanced communications service" under section 1.50001(a), this would encompass any equipment that can be used in such a fixed or mobile broadband network to enable users to originate and receive high quality voice, data, graphics, and video telecommunications using technology with connection speeds of at least 200 kbps in either direction.[472] By taking this broad approach,[473] we bring within the scope of our prohibition a wide range of communications equipment that are used within broadband networks. Our goal in adopting this definition is to provide clear guidance that promotes regulatory compliance and administrability, as well as regulatory certainty.[474]

---

[469] *Id.* at 10603-04, para. 57.

[470] *See, e.g., Supply Chain 2nd R&O*, 35 FCC Rcd at 14308, para. 52. In defining "communications equipment" that is "essential to the provision of advanced communications service" under the Secure Networks, Act, the Commission defined the term broadly to mean "any equipment … used in fixed or mobile networks that provides advanced communications service, provided the equipment … includes or uses electronic components." The Commission expressed its belief that all equipment that includes or uses electronic component can "reasonably be considered essential to broadband networks." *See id.* Furthermore, in defining "advanced communications service," the Commission again took a broad, more inclusive approach to ensure that the definition covers a broad array of equipment and services, including older legacy technology. The Commission found this broader approach "consistent with congressional intent to identify and remove insecure equipment." *Id.* at 14310-11, para. 55.

[471] *See* 47 CFC § 1.50001(c) (the definition of "communications equipment or service" for purposes of implementing the Secure Networks Act).

[472] *See id.* § 1.50001(a) (the definition of "advanced communications service" for purposes of implementing the Secure Networks Act).

[473] We note that Motorola agrees with this approach. Motorola Mar. 24, 2022 *Ex Parte* at 4 (contending that any equipment that can be used in a fixed or mobile broadband network to enable "users to originate and receive high quality voice, data, graphics, and video telecommunications using any technology with connection speeds of at least 200 kbps in either direction" would be "covered").

[474] *See Supply Chain 2nd R&O*, 35 FCC Rcd at 14308, paras. 52-53.

196. We reject the contention that "telecommunications equipment" under the Secure Networks Act must necessarily exclude all CPE equipment or IoT equipment,[475] or that "telecommunications equipment" under the Secure Networks Act should be defined in the same manner as the term "telecommunications equipment" is defined under the Communications Act.[476] In interpreting and broadly defining "communications equipment" under the Secure Networks Act, the Commission indicated its concern, consistent with congressional intent, that the Commission protect against the use of insecure equipment in advanced communications services, and it did not indicate an intent to exclude all CPE or IoT equipment from the scope of "covered" equipment under the Act.[477] Nor was there any indication by Congress, when adopting section 889(f)(3) as part of the NDAA of 2019 regarding prohibitions on federal agencies' procurement of "telecommunications equipment" (or "video surveillance equipment") that the term "telecommunications equipment" in the NDAA was to be narrowly defined and limited to "telecommunications equipment" as defined in the Communications Act or used by the Commission in certain Commission-focused contexts. As Motorola points out, the NDAA involves a different statutory scheme.[478] As the courts have repeatedly recognized, Congress may have intended to accord different scope to the same language used in different statutes, depending upon the context and purpose of the statutory scheme.[479] Indeed, we note that the federal agencies' own procurement rules, whose national security purposes are much more relevant here, define "telecommunications" broadly as "the transmission, emission, or reception of signals, signs, writing, images, sounds, or intelligence of any nature, by cable, satellite, fiber optics, laser, radio, or other electronic, electric, electromagnetic, or acoustically coupled means;" those rules further define "telecommunications services" as meaning "the services acquired, whether by lease or by contract, to meet the Government's telecommunications needs," including "the *equipment* necessary to provide such

[475] *See, e.g.*, Hikvision USA Nov. 17, 2021 *Ex Parte* at 5 (handsets and other customer premises equipment, including IOT devices that utilize advanced communications services, are distinctly different from core networks, and therefore not "covered"); Dahua USA Jan. 4, 2022 *ex parte* at 2 (Commission is neither authorized to exclude all Dahua equipment from the equipment authorization process under part 2 of the Commission's rules, nor to subject Dahua USA's peripheral IoT non-communications equipment to discriminatory treatment under those rules). Hikvision USA argues, in particular, that the Commission in its *Supply Chain 3rd R&O* acknowledged that handsets and other consumer premises equipment, including IOT devices – the types of devices that Hikvision contends include its video surveillance equipment – are used to access and utilize advanced communications services but are distinctly different from cell sites, backhaul, and core network. Hikvision USA Nov. 17, 2021 *Ex Parte* at 4-5 (citing *Supply Chain 3rd R&O*, 36 FCC Rcd at 11996, para. 94).

[476] Hytera Ltd., Hytera USA, and PowerTrunk June 3, 2022 *Ex Parte* at 2. *See also* Hytera Ltd., Hytera USA, and PowerTrunk Aug. 17, 2021 *Ex Parte*, Slide Presentation at 8 (citing section 153(22) of the Communications Act of 1934, as amended (defining the term "telecommunications equipment" as meaning equipment, other than customer premises equipment, used by a carrier to provide telecommunications services).

[477] We note that we are not limited in this equipment authorization proceeding to the particular equipment that the Commission determined would be eligible for reimbursement under the Reimbursement Program. As discussed in the *Supply Chain 3rd R&O*, in implementing the Consolidated Appropriations Act of 2021 amendments to the Secure Networks Act, the Commission expressly limited that Reimbursement Program to only a subset of the Covered List, specifically limiting that program to Huawei and ZTE equipment. *Supply Chain 3rd R&O*, 36 FCC Rcd at 11966-67, 11669-70, paras. 22-23, 29. The Commission noted that that Reimbursement Program excluded "covered" equipment produced by Hytera, Hikvision, and Dahua, as identified on the Covered List. *Id.* at 19670, para. 29 n.90.

[478] Motorola Reply at 12-13.

[479] *See Fogerty v. Fantasy, Inc.*, 510 U.S. 517, 522-25 (1994) (interpreting nearly identical language in the Copyright Act and Title VII of the Civil Rights Act differently based, in part, on the differing objectives of the two Acts); *Eddy v. Colonial Life Ins. Co. of America*, 59 F.3d 201, 205-206 (1995) (distinguishing similar language in several civil rights statutes and ERISA based on the divergent goals of the statutes and the legislative history); *see also American Council on Education v. FCC*, 451 F.3d 226, 233-34 (D.C. Cir. 2006) (upholding the Commission's determination that "telecommunications service" in CALEA could be more extensive than the same term in the Communications Act).

services" (emphasis added).[480] Considering our goal of eliminating future authorization of "covered" equipment that poses an unacceptable risk to national security, we do not interpret the scope of "covered" equipment narrowly because a limited view of what constitutes insecure equipment would potentially result in an unacceptable risk to national security and would be inconsistent with the broader definition used by federal agencies implementing the section 889 prohibition on federal agency procurement of "telecommunications equipment."

197. We also note, for instance, that pursuant to section 5 of the Secure Networks Act the Commission requires that advanced communications service providers submit annual reports certifying whether they had purchased, leased, rented, or otherwise obtained "covered" equipment after August 18, 2018.[481] The Commission directed the Office of Economics and Analytics (OEA) to administer this data collection,[482] and in doing so it issued guidance ("Supply Chain Annual Reporting 2022 Filing Instructions") to define the information that advanced service providers were required to file and to act as a guide to assist filers with submitting the necessary information.[483] Pursuant to these instructions, advanced service providers are required to submit information on "covered" equipment that is in different layers of their networks, including in the "access layer," the "distribution layer," and the "core layer."[484] "Access layer" equipment is equipment associated with providing and controlling end-user access to the network over the "last mile," "local loop," or "to the home" (e.g., optical terminal line equipment, optical distribution network devices, customer premises equipment (to the extent owned by the advanced services provider), coaxial media converters, wavelength-division multiplexing (WDM) and optical transporting networking (OTN) equipment, and wireless local area network (WLAN) equipment). "Distribution equipment" includes middle mile, backhaul, and radio area network (RAN) equipment (e.g., routers, switches, network security equipment, WDN and OTN equipment, and small cells).[485] "Core layer" equipment is associated with the backbone infrastructure (e.g., optical networking equipment, WDN and OTN, microwave equipment, antennas, RAN core, Cloud core, fiber, and data transmission equipment).[486] We affirm the broad approach taken by OEA in implementing the annual reporting requirement on "covered" equipment – including its specific inclusion of "access layer," "distribution layer," and "core layer" equipment in networks providing advanced communications services as falling within the scope of what constitutes "covered" equipment under the Secure Networks Act.

198. Because of the wide array and variety of devices in the marketplace, we cannot in this Report and Order identify all of the categories or types of equipment that would constitute

---

[480] The Federal Acquisition Regulations System regulations includes a definition on "telecommunications services," which includes the "equipment necessary to provide such services." *See* 48 CFR § 239.7401 ("Definitions").

[481] *Supply Chain 2nd R&O*, 35 FCC Rcd at 14369, para. 212; 47 CFR § 1.50007.

[482] *Supply Chain 2nd R&O*, 35 FCC Rcd at 14370, para. 215.

[483] *Supply Chain Annual Reporting 2022 Filing Instructions*, found at https://www.fcc.gov/sites/default/files/supply_chain_annual_reporting_instructions.pdf. *See id.* at 3 ("Purpose").

[484] *See id.* at 25. These instructions provide also provide definitions and further information regarding these network layers. *Id.* (citing "Protecting the Communications Supply Chain, Information Collection, Network Categories" found at https://us-fcc.app.box.com/v/NetworkCategories).

[485] *See Supply Chain Annual Reporting 2022 Filing Instructions* at 25; "Protecting the Communications Supply Chain, Information Collection, Network Categories," https://us-fcc.app.box.com/v/NetworkCategories.

[486] We also note that the Commission had directed the Wireline Competition Bureau (WCB), in implementing the Secure Networks Act Reimbursement Program to develop a "Catalog of Expenses Eligible for Reimbursement." *Supply Chain 2nd R&O*, 35 FCC at 14339-40, paras. 128-29; *see* 47 CFR § 1.50004(p). The catalog ultimately developed by WCB and published on the Commission's website similarly identified categories of equipment – including Huawei and ZTE equipment in the "access layer," the "distribution layer," and the "core layer" of a communications network – that would be eligible for purposes of reimbursement under the Reimbursement Program. *See Final Catalog of Eligible Expenses and Estimated Costs* (Revised December 17, 2021), found at https://www.fcc.gov/sites/default/files/scrp-final-catelog-eligible-expenses-estimated-costs-12172021.pdf.

"telecommunications equipment." We nonetheless proffer some additional clarity consistent with our broad definition of "telecommunications equipment" for purposes of implementing our prohibition on authorization of "covered" equipment in this proceeding.

199. Huawei and ZTE each produce, among other things, different types of equipment that requires certification, including base stations, cell phone and smart phone handsets, tablets, and routers that operate under particular rules for licensed services (e.g., part 22, 24, 27, 90, 96) as well as various unlicensed devices, including Wi-Fi routers. Hytera produces, among other things, base station units and repeaters, as well as trunking systems PLMR/DLMR handsets and two-way radios,[487] which operate under various rules for licensed services (e.g., part 22, 24, 80, 90, 95). Hytera representatives assert not only that Hytera equipment is not "covered" because it is "peripheral" equipment or CPE, but also contend generally that Hytera equipment is not "telecommunications equipment" or "covered communications equipment" because it is generally not interconnected to a fixed or mobile broadband network[488] (although its notes that a small subset of handsets (e.g., PowerTrunk TETRA) is so designed[489]). As noted above, Hikvision and Dahua representatives also each generally assert the company does not produce any "telecommunications equipment," and argue that no CPE and IoT can be deemed such equipment.[490] Hikvision USA further asserts that, while Hikvision does produce U-NII router equipment for unlicensed use, such equipment is not "covered" because it is CPE and is within an end-user's internal enterprise network on the user's side of the gateway router and therefore not broadband equipment.[491]

200. Whether particular equipment is covered telecommunications equipment will turn on applying the Commission's interpretation of what constitutes such equipment as discussed above. We note that Motorola supports a broad interpretation concerning telecommunications equipment consistent with the approach described above, i.e., that encompassed within the scope of "covered" equipment is equipment that "enable users to originate and receive high quality voice, data, graphics, and video telecommunications with connection speeds of at least 200 kbps in either direction."[492] Responding to Motorola, Dahua USA contends that such a broad definition is not statutorily permissible under the Secure Networks Act and would include, for instance, Wi-Fi connected household appliances, such as a smart oven, or IoT devices such as LED lightbulbs or digital clocks;[493] Motorola disagrees, stating that its interpretation would not make prohibit those devices because such equipment does not enable users to originate and receive high quality voice, data, graphics, and video communications using technology at the applicable connection speeds.[494] Meanwhile, Hytera US asserts that its PLMR equipment does not have the capability to enable users to originate and receive high quality voice, data, graphics, or video telecommunications of at least at 200 kbps.[495] Motorola disputes the contention that most of the Hytera

[487] *See, e.g.*, Hytera Ltd. and PowerTrunk Aug. 17, 2021 *Ex Parte* at 1; Hytera US Apr. 1, 2022 *Ex Parte* at 3

[488] *See, e.g.*, Hytera Ltd. and PowerTrunk Aug. 17, 2021 *Ex Parte* at 1.

[489] Hytera US June 3, 2022 *Ex Parte* at 2.

[490] *See, e.g.*, Hikvision USA Nov. 17 *Ex Parte* at 5; Dahua USA Jan. 4, 2022 *Ex Parte* at 2.

[491] Hikvision USA June 29, 2022 *Ex Parte* at 2.

[492] Motorola Mar. 24, 2022 *Ex Parte* at 4.

[493] Dahua USA Apr. 7, 2022 *Ex Parte* at 9-10.

[494] Motorola May 3, 2022 *Ex Parte* at 6 (quoting the Commission's definition of "advanced communications service" at 47 CFR § 1.50001(a)). Motorola specifically disputes Dahua USA's claim in its April 7 *Ex Parte* that Motorola's interpretation approach is too expansive and has no limiting principle. *Id.* *See* Dahua Apr. 7, 2022 *Ex Parte* at 9-10.

[495] *See, e.g.*, Hytera US Apr. 1, 2022 *Ex Parte* at 3.

radio equipment is narrowband since it can utilize a broadband service, noting that Hytera's US website indicates that many of its radios combine narrowband communications with LTE broadband data input.[496]

201. As discussed above, we believe that Congress intended to take a broad view of what constitutes "covered" "telecommunications equipment" for purposes of our prohibition on future equipment authorizations. Accordingly, we conclude not only that the types of "telecommunications equipment" specifically identified in the Supply Chain Annual Reporting 2022 Filing Instructions are "covered" for the purposes of this proceeding, including equipment such as cellular base stations, backhaul, and core network equipment, but we also clarify that handsets designed for operation over fixed or mobile networks providing advanced communications services also are "covered." We make this decision recognizing that handsets generally, as well as many CPE and IoT devices, meet the broad definition we adopt here insofar as these devices incorporate electronic components, could enable users to originate and receive high quality voice, data, graphics, and video telecommunications with connection speeds of at least 200 kbps in either direction, and may be the end points of most broadband networks which makes them part of the network. We disagree with Hikvision USA's suggestion that the Commission has already concluded in the *Supply Chain 3rd R&O* that handsets, CPE, and IoT necessarily are not "covered" equipment when it observed that handsets and other CPE including IoT used by end users are different from cell sites, backhaul and core network equipment and then declined to require that such equipment be removed, replaced, and reimbursed under the Reimbursement Program.[497] That observation only addressed what equipment would be eligible for reimbursement under the Reimbursement Program, and was not intended to define the nature of what equipment should be considered "covered." As Motorola rightly notes,[498] and as we point about above, that proceeding limited the scope of the Reimbursement Program to a subset of the Covered List, and the equipment and services on the Covered List was not at issue.[499] In our equipment authorization program, we are not concerned with the Reimbursement Program but instead are focused on preventing future authorization of equipment that could pose an unacceptable risk to national security or the security and safety of U.S. persons. We conclude that handset equipment designed for operation over broadband networks and that enable users to originate and receive high quality voice, data, graphics, and video telecommunications with connection speeds of at least 200 kbps in either direction fall within the broad scope of our interpretation of "telecommunications equipment" and is "covered." Accordingly, we note that Huawei and ZTE handsets, and Hytera handsets to the extent designed to operate over broadband networks, are "covered."[500] We also note that this approach fully accords with congressional intent in the Secure Equipment Act, in which Congress sought to ensure that the Commission not approve devices that pose a national security risk and that equipment for which public funding was prohibited because it poses an unacceptable risk also should be addressed in the equipment authorization program.[501] As for other CPE or IoT devices, whether particular equipment is "covered" will depend on whether it meets the requirements for "covered" equipment discussed above. These terms have been defined by industry in a variety of ways and contexts, and could include a wide range of equipment and technologies that may connect to the internet or other broadband networks without any specific regard as to whether the equipment would meet the

[496] Motorola May 3, 2022 *Ex Parte* at 5 & n.21.

[497] *See, e.g.*, Hikvision USA May 27, 2022 *Ex Parte* at 2 (citing *Supply Chain 3rd R&O*, 36 FCC Rcd at 11996, para. 94).

[498] Motorola May 3, 2022 *Ex Parte* at 6-7.

[499] As we previously discussed, the Commission's Reimbursement Program, established by section 4 of the Secure Networks Act, as amended, is limited to Huawei and ZTE equipment and services obtained on or before June 30, 2020. This equipment authorization proceeding is concerned with the Covered List, which has a broader scope than the Reimbursement Program.

[500] We note that if Hikvision or Dahua produce "telecommunications equipment" that are handsets, then such equipment also would be "covered."

[501] Report to accompany H.R. 3919, the Secure Equipment Act of 2021, Report 117-148, at 1.

requirements of "covered" communications equipment under the Secure Networks Act as interpreted by the Commission (e.g., enable users to originate high quality voice, data, graphics, and video telecommunications with connection speeds of at least 200 kbps in either direction).

202. Because the Commission authorizes a wide range of equipment, and because additional clarification on "covered" equipment may be needed, we delegate to OET and PSHSB, working with WTB, IB, WCB, EB and OGC as appropriate, to develop and finalize additional clarifications as needed to inform applicants for equipment authorization, TCBs, and other interested parties with more specificity and detail on the categories, types, and characteristics of equipment that constitutes "telecommunications equipment" for purposes of the prohibition on future authorization of "covered" equipment identified on the Covered List. As we note above, federal agencies are actively engaged in prohibiting procurement of "covered" equipment, including "telecommunications equipment" as defined by section 889(f)(3) of the 2019 NDAA.[502] As OET and PSHSB develop more detailed guidance for purposes of the prohibition in our equipment authorization program, they may also review efforts from other federal agencies, such as the General Services Administration's efforts in its implementation of the procurement prohibition and the types of "telecommunications equipment" that constitute such "covered" equipment, the Federal Acquisition Security Council,[503] the Department of Homeland Security's Information and Communications Supply Chain Risk Management Task Force,[504] or other federal efforts, if those efforts are relevant to development of the guidance.[505]

203. We further direct OET and PSHSB to issue future clarifications in a Public Notice, and to post these clarifications on the Commission's website for ready access by all interested parties. This guidance will serve as a reference for applicants and other stakeholders to provide consistency and clarity for purposes of complying with our rules prohibiting authorization of "covered" equipment. OET and PSHSB are further directed to provide updated clarifications as appropriate, which could be further informed by information provided by interested parties. We are also requiring that a Public Notice be issued with any updates to the guidance, along with an updated website. This guidance also can be used to assist TCBs in their assessments of equipment authorization applications to help preclude authorization of any "covered" equipment.

204. *Video surveillance equipment.* As with "telecommunications equipment," considering the importance of prohibiting authorization of "covered" equipment that poses an unacceptable risk to national security, we broadly interpret "video surveillance equipment" under the Secure Networks Act and section 889(f)(3) of the 2019 NDAA for purposes of the Commission's equipment authorization program. As discussed above, taking a broad approach to defining "covered" equipment also is consistent with our earlier decisions defining "covered" equipment broadly under the Secure Networks Act, and is in accord with congressional intent set forth in the Secure Equipment Act.

205. In particular, we interpret "video surveillance equipment," consistent with the definition in our rules concerning "communications equipment" under the Secure Networks Act,[506] to include any equipment that is used in fixed and mobile networks that provides advanced communications service in the form of a video surveillance service, provided the equipment includes or uses electronic components.

---

[502] See paragraph 13, *supra.*

[503] The Federal Acquisition Security Council was established pursuant to the SECURE Technology Act. *See* P.L. 115-390, 132 Stat. 5173, https://www.congress.gov/115/bills/hr7327/BILLS-115hr7327enr.pdf.

[504] The Information and Communications Technology Supply Chain Risk Management Task Force is a public-private supply chain risk management partnership established in to identify and develop consensus strategies that enhance supply chain security. *See* https://www.cisa.gov/ict-scrm-task-force.

[505] We note that the Commission similarly authorized WCB to review relevant efforts of federal agencies as WCB developed guidance for identifying equipment that would need to be removed and replaced under the Reimbursement Program. *Supply Chain 2nd R&O*, 35 FCC Rcd at 14365-36, para. 201.

[506] *See* 47 CFR § 1.50001(c).

In keeping with the definition of "advanced communications service,"[507] we intend with this definition to encompass all equipment that is designed and capable for use for purposes of enabling users to originate and receive high-quality video telecommunications service using any technology with connection speeds of at least 200 kbps in either direction.

206. As discussed, Hikvision and Dahua each produce a wide range of products that are associated with video surveillance capabilities, including cameras, video recorders, and network storage devices. Although Hytera asserts that it does not produce any video surveillance equipment, we note that among other things it manufactures "body-worn camera" equipment.[508] In their submissions, Hikvision and Dahua representatives each contend that its video surveillance equipment is "peripheral" or CPE, and hence not "covered."[509] We reject that view altogether, particularly given that section 889(f)(3) specifically discusses "video surveillance equipment" as "covered," which reflects Congress's clear intent that video surveillance equipment can pose an unacceptable risk to national security.[510] Hikvision and Dahua representatives also contend their respective video surveillance equipment is not "covered" because the equipment does not require connection to the internet (an end user's choice);[511] Hikvision USA does acknowledge, however that some of its video surveillance equipment (HikConnect) does require internet connection,[512] and that in any event its equipment poses no danger because it is secure.[513] Dahua USA contends, among other things, that its digital video recorders, network video recorders, data storage devices, and video surveillance servers should not be deemed "covered."[514] IPVM asserts that most video surveillance equipment today has internet connectivity as a widely-demanded feature,[515] and notes in particular that Hikvision surveillance cameras are generally marketed as Internet-protocol (IP) cameras that are designed and marketed for use connected to internet.[516] IPVM also disagrees with Dahua USA's contention that video recorders are not "covered" as "video surveillance equipment,"[517] and generally contends broadly that Hikvision and Dahua equipment poses a threat to the American public.[518] Given the concerns Congress raised about the potential risks to national security associated with such video surveillance capabilities, we believe it intended to take the broad view on what constitutes video surveillance equipment, and conclude that it includes not only surveillance cameras, but also video

[507] 47 CFR § 1.50001(a) ("'advanced communication service' means high-speed, switched broadband communications capability that enables users to originate and receive … video telecommunications …").

[508] We note that the Hytera US website posts information on Hytera's "Body-worn Camera," which it states "allows users to communicate efficiently, initiate emergency alarm, and deliver real-time video to a control center over the LTE network." *See, e.g.*, https://www.hytera.us/products/vm682-bodycam-radio?utm_term=&utm_campaign=US+Google+H-Series+Performance+Max+Display&utm_source=adwords&utm_medium=ppc&hsa_acc=9676105482&hsa_cam=17382021597&hsa_grp=&hsa_ad=&hsa_src=x&hsa_tgt=&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ver=3&gclid=EAIaIQobChMIuJnb_-DC-gIVBL_ICh1esQl4EAAYAiAAEgL9svD_BwE (viewed on October 2, 2022).

[509] *See, e.g.,* Hikvision USA May 27, 2022 *Ex Parte* at 3; Dahua USA Dec. 10, 2021 *Ex Parte*, Slides at 4.

[510] *See* Section 889(f)(3)(B)-(C).

[511] *See, e.g.*, Hikvision USA Feb. 23, 2022 *Ex Parte* at 3-4 (noting that the end-user can choose and contending that most users choose not to interconnect); Dahua USA May 27, 2022 *ex parte* at 2.

[512] *See, e.g.*, Hikvision USA Feb. 23, 2022 *Ex Parte* at 4.

[513] *See, e.g.*, *id,*; Dahua USA Reply Comments at 10-11.

[514] Dahua USA June 28, 2022 *ex parte* at 4 & Appendix A (listing equipment Dahua contends is "not" covered "video surveillance" or "telecommunications equipment").

[515] *See, e.g.*, IPVM Feb. 7, 2022 *Ex Parte* at 1.

[516] IPVM Feb. 7, 2022 *Ex Parte* at 1-3; *see generally* IPVM Mar. 24, 2022 *Ex Parte*.

[517] *See generally* IPVM Aug. 11, 2022 *Ex Parte*.

[518] *See, e.g.*, IVPM Reply Comments at 1.

surveillance equipment associated with video surveillance services that make use of broadband capabilities, such as video recorders, video surveillance servers, and video surveillance data storage devices. We make this determination recognizing that these devices are capable of storing and sharing their content over broadband networks and thus being connect to the network, they become part of the network. We also conclude that Hytera equipment that includes capabilities associate with video surveillance service, such as "body cams," which are generally designed to connect to the internet, also is "video surveillance equipment" that is "covered."

207. As with "telecommunications equipment," we delegate to OET and PSHSB, working with WTB, IB, WCB, EB and OGC as appropriate, to develop and finalize additional guidance to inform applicants for equipment authorization, TCBs, and other interested parties in more specificity and detail information on the categories, types, and characteristics of equipment that constitutes "video surveillance equipment." As the OET and PSHSB develop further clarification, we authorize them also to review efforts from other federal agencies, such as the General Services Administration's efforts in its implementation of the procurement prohibition and the types of "video surveillance equipment" that constitute such "covered" equipment under section 889(f)(3), the Federal Acquisition Security Council,[519] the Department of Homeland Security's Information and Communications Supply Chain Risk Management Task Force,[520] or other federal efforts, if those efforts are relevant to development of further clarification on what constitutes "covered" equipment.[521]

208. *For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes.* Pursuant to the Secure Networks Act and section 889(f)(3)(B) of the NDAA of 2019, we are prohibiting, as "covered" equipment, the authorization of any "telecommunications equipment" or "video surveillance equipment" produced by Hytera, Hikvision, and Dahua (or their subsidiaries and affiliates) "[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes."[522] As with "telecommunications equipment" and "video surveillance equipment," we interpret the scope of this section 889(f)(3)(B) prohibition broadly given the importance of preventing "covered" equipment from being made available for prohibited uses that would pose an unacceptable risk to national security or the security of U.S. persons.

209. In particular, we construe the scope of elements associated with these purposes – public safety, government facilities, critical infrastructure, and national security – broadly with respect to the implementation in our equipment authorization program of the prohibition concerning "covered" Hytera, Hikvision, and Dahua equipment pursuant to the Secure Networks Act and section 889(f)(3)(B) of the 2019 NDAA. We interpret the phrase "[f]or the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes" broadly, i.e., as having broad scope with respect to any prohibition relating to covered communications equipment. Terms comprising this phrase – public safety, government facilities, critical infrastructure, and national security – are each construed broadly in order to prohibit authorization of equipment that poses an unacceptable risk to national security of the United States or to the security or safety of U.S. persons. We discuss each of these terms below, and how we broadly construe them consistent with the

[519] The Federal Acquisition Security Council was established pursuant to the SECURE Technology Act. *See* P.L. 115-390, 132 Stat. 5173, https://www.congress.gov/115/bills/hr7327/BILLS-115hr7327enr.pdf.

[520] The Information and Communications Technology Supply Chain Risk Management Task Force is a public-private supply chain risk management partnership established in to identify and develop consensus strategies that enhance supply chain security. *See* https://www.cisa.gov/ict-scrm-task-force.

[521] We note that the Commission similarly authorized WCB to review relevant efforts of federal agencies as WCB developed guidance for identifying equipment that would need to be removed and replaced under the Reimbursement Program. *Supply Chain 2nd R&O*, 35 FCC Rcd at 14365-36, para. 201.

[522] Section 889(f)(3)(B).

Secure Networks Act, section 889(f)(B) of the NDAA, and our goals in this proceeding to protect national security and the security and safety of U.S. persons.

210. With respect to "public safety," we find that this includes services provided by State or local government entities, or services by non-governmental agencies authorized by a governmental entity if their primary mission is the provision of services, that protect the safety of life, health, and property, including but not limited to police, fire, and emergency medical services.[523] For purposes of implementing the Secure Networks Act and the Secure Equipment Act, we interpret public safety broadly to encompass the services provided by Federal law enforcement and professional security services, where the primary mission is the provision of services, that protect the safety of life, health, and property. We believe that this best fulfills Congress' intent with respect to the scope of public safety as that term is used in section 889(f)(3) in connection with "covered" Hytera, Hikvision, and Dahua equipment and the other terms in that section.

211. With respect to the term "government facilities," we find instructive the Cybersecurity and Infrastructure Security Agency's (CISA) view of what constitutes the government facilities sector. According to CISA, the government facilities sector includes "a wide variety of buildings, located in the United States and overseas, that are owned or leased by federal, state, local, and tribal governments."[524] In addition to facilities that are open to the public, CISA notes that others "are not open to the public [and] contain highly sensitive information, materials, processes, and equipment," and that these facilities include and are not limited to "general-use office buildings and special-use military installations, embassies, courthouses, national laboratories, and structures that may house critical equipment, systems, networks, and functions."[525] CISA also notes that "[i]n addition to physical structures, the sector includes cyber elements that contribute to the protection of sector assets (e.g., access control systems and closed-circuit television systems) as well as individuals who perform essential functions or possess tactical, operational, or strategic knowledge."[526] We believe that this description provides ample guidance for purposes of what constitutes "government facilities" for implementation of the prohibition that we adopt today.

212. With regard to scope of "critical infrastructure" and the prohibition that we are adopting in this proceeding, we apply the meaning provided in section 1016(e) of the USA Patriot Act of 2001, namely, "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[527] Presidential Policy Directive 21 (PPD-21) identifies sixteen critical infrastructure sectors: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, health care and public health, information

[523] *See* 47 U.S.C. § 337(f)(1). *See also, e.g.,* 47 CFR § 90.16 (establishing a Public Safety National Plan which specifies policies and procedures governing the Public Safety Pool); *Development and Implementation of a Public Safety National Plan and Amendment of Part 90 to Establish Service Rules and Technical Standards for Use of the 821-824/866-869 MHz Bands by the Public Safety Services*, GN Docket No. 87-112, Report and Order, 3 FCC Rcd 675, 905, para. 1 (1987) (This National Plan ... will ensure that the new channels are used effectively and efficiently for important public safety functions such as crime control, firefighting, and emergency medical services.").

[524] *Government Facilities Sector*, https://www.cisa.gov/government-facilities-sector, (last visited Sept. 21, 2022).

[525] *Id.*

[526] *Id.*

[527] 42 U.S.C. § 5195c(e)). *See also* Directive on Critical Infrastructure Security and Resilience, 1 Pub. Papers 106, 115 (Feb. 12, 2013) [hereinafter PPD-21], https://www.govinfo.gov/content/pkg/PPP-2013-book1/pdf/PPP-2013-book1-doc-pg106.pdf; Homeland Security Presidential Directive on Critical Infrastructure Identification, Prioritization, and Protection, 2 Pub. Papers 1739, 1739 (Dec. 17, 2003) [hereinafter HSPD-7], https://www.govinfo.gov/content/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1739.pdf.

technology, nuclear reactors/materials/waste, transportation systems, and water/waste water systems.[528] In this connection, CISA, through the National Risk Management Center (NRMC), published a set of 55 National Critical Functions (NCFs) to guide national risk management efforts.[529] The CISA/NRMC guide defines "critical infrastructure" similar to how that term is defined in the USA Patriot Act. Specifically, it defines the NCFs as "functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[530] For purposes of implementing the rules we are adopting today, we find that any systems or assets, physical or virtual, connected to the sixteen critical infrastructure sectors identified in PPD-21 or the 55 NCFs identified in CISA/NRMC could reasonably be considered "critical infrastructure."

213. As for "national security," for purposes of this proceeding, we interpret this term broadly as encompassing a variety of high-profile assets involving government, commercial, and military assets. In this connection, we note that section 709(6) of the Intelligence Authorization Act for Fiscal Year 2001, provides that "'national security' means the national defense or foreign relations of the United States."[531] Accordingly, we will rely on this definition for guidance.

214. We delegate to OET and PSHSB, working with WTB, IB, WCB, EB and OGC as appropriate, to develop further clarifications to inform applicants for equipment authorization, TCBs, and other interested parties with more specificity and detail. As the Commission develops more detailed guidance, we authorize OET and PSHSB also to review efforts from and coordinate as necessary with our federal partners, such as but not limited to the Department of Justice, Department of Commerce, Department of Homeland Security, and Federal Bureau of Investigation.

215. *Declaratory ruling.* To the extent an interested party may seek to clarify whether particular equipment is "covered" for purposes of the equipment authorization prohibition, it can bring a request for declaratory ruling before the Commission. We note that the Commission, in its 2020 *Supply Chain 2nd R&O*, similarly noted that any interested party that may seek to clarify whether a specific piece of equipment is included as "covered" on the Covered List could seek a declaratory ruling.[532] At the same time, we note again that the Commission has no discretion to reverse or modify determinations from the four enumerated sources under the Secure Networks Act that are responsible for those determinations, which the Commission must accept and include on the Covered List as provided, and that should a party seek to reverse or modify any such determination it should petition the source of the determination.[533] Moreover, the seeking of clarification by any party does not entitle such party to any presumption, nor is it the basis for arguing, that specific equipment is not "covered," absent additional clarification from the Commission. We delegate to OET and PSHSB authority to issue such declaratory rulings consistent with principle of broad interpretation of terms given the importance of preventing "covered" equipment from being made available for prohibited uses that would pose an unacceptable risk to national security or the security of U.S. persons, as illustrated above.

---

[528] PPD-21, at 114-15.

[529] National Risk Management Center, Cybersecurity and Infrastructure Security Agency, National Critical Functions Status Update to the Critical Infrastructure Community (2020), https://www.cisa.gov/sites/default/files/publications/ncf-status-update-to-critical-infrastructure-community_508.pdf.

[530] *Id.* at 1.

[531] 50 U.S.C. 3355g(6),https://www.govinfo.gov/content/pkg/PLAW-106publ567/pdf/PLAW-106publ567.pdf .

[532] *Supply Chain 2nd R&O*, 35 FCC Rcd at 14323-34, para. 88.

[533] *Id.* at 14324, para. 89.

6. Future updates on "covered" equipment and the Covered List

216. As noted, we anticipate that the Covered List, which was most recently updated and published on September 20, 2022,[534] will continue to be revised in the future based on further determinations about communications equipment made by any one of the four enumerated sources that are identified in section 2(c) of the Secure Networks Act. As discussed above, to date the only determination that specifically concerns communications equipment is that made under section 2(c)(3) of the Secure Networks Act, specifically the determination made by Congress in section 889(f) of the 2019 NDAA. Future determinations concerning communications equipment could involve determinations by any of the other three enumerated sources as specified under the Secure Networks Act – per section 2(c)(1), "[a] specific determination made by any executive branch interagency body with appropriate national security expertise, per including the Federal Acquisition Security Council established under section 1322(a) of title 41, United States Code; per section 2(c)(2), "[a] specific determination made by the Department of Commerce pursuant to Executive Order No. 13873 (84 Fed. Reg. 22689; relating to securing the information and communications technology and services supply chain); and per section 2(c)(4), "[a] specific determination made by an appropriate national security agency."[535]

217. As noted above, the Commission is required to monitor the status of determinations in order to update the Covered List by modifying, adding, or removing "covered" equipment on the Covered List, pursuant to section 1.50003.[536] Under the rules adopted herein, the Commission will no longer authorize for marketing or sale equipment that has been placed on the Covered List, as that list evolves.

218. The Commission guidance provided in this Report and Order, along with the delegation of authority directing OET and PSHSB to publish and maintain information on the Commission's website concerning "covered" equipment should serve to enable implementation of updates concerning equipment that are placed on the Covered List. We note, for instance, that a new determination might modify the "covered" equipment on the Covered List only with regard to adding or removing the named entities that produce equipment that poses an unacceptable risk to national security. If so, then the guidance on the Commission's website can readily by updated on delegated authority and the added equipment will be prohibited in our equipment authorization program. We recognize, however, that a future determination by one of the four enumerated sources that results in an updated Covered List with respect to new types of equipment that pose an unacceptable risk potentially could require further consideration on delegated authority, consistent with the approach discussed above; if so, we direct OET and PSHSB to so indicate through Public Notice, including discussion of the process by which the guidance will be developed and provided.

D. Other Issues

1. Cost-effectiveness and economic impact

219. In the *NPRM*, the Commission stated that its proposed revisions to the Commission's equipment authorization rules and processes to prohibit authorization of "covered" equipment that had been determined by any one of the four enumerated source outside of the Commission as posing an unacceptable risk to national security would not be subject to a conventional cost-benefit analysis.[537] The Commission stated that because it has no discretion to ignore these determinations, a conventional cost-benefit analysis – which would seek to determine whether the costs of the proposed actions would exceed the benefits – is not directly called for. Instead, the Commission stated that it would consider whether its actions would be "a cost effective" means to prevent this dangerous equipment from being introduced

[534] *September 2022 Covered List Public Notice*.

[535] Secure Networks Act, § 2(b)-(c).

[536] 47 CFR § 1.50003.

[537] *NPRM*, 36 FCC Rcd at 20698, paras. 70-71.

into our nation's communications networks, and sought comment on the Commission's proposed revisions to the equipment authorization rules and procedures.[538]

220. Several commenters assert that the Commission should engage in a cost-benefit analysis as it considers adoption of rules concerning the prohibition of authorization of "covered" equipment.[539] Several also discussed the potential for unintended consequences to the supply chain.[540] For instance, Hikvision claims that a prohibition on video surveillance equipment would be disruptive to American businesses[541] and burdensome to consumers.[542] Dahua USA argues that the proposed rules are not cost-effective, would have a negative impact on the U.S. economy, and would add extra administrative burdens on the Commission and market participants.[543] IVPM, however, says that there are at least 40 video surveillance equipment alternatives to video surveillance equipment on the Covered List.[544]

221. We recognize that adopting a prohibition on the authorization of "covered" equipment may result in economic impacts on entities directly or indirectly associated with the "covered" equipment identified on the Covered List. However, as we note above, the rules adopted in this Report and Order regarding future authorizations of "covered" equipment are mandated by the Secure Equipment Act, requiring that the Commission will not approve any application for equipment authorization for equipment that is on the Covered List.[545] The equipment included on the Covered List was determined by other expert agencies as posing an unacceptable risk to national security. As noted in the *NPRM*, because the Commission has no discretion to ignore the congressional mandates and other expert agencies' determinations, we find that a full cost-benefit analysis is not required with respect to the actions that the Commission is taking in the Report and Order. Moreover, as we explain below, we find that the rules that we adopt herein are a cost-effective approach to carry out the requirements of the Secure Equipment Act.

222. *Certification rules and procedures*. We find that our revision of section 2.911 requiring that applicants for equipment authorizations in the certification process attest that their equipment is not "covered" equipment on the Covered List while also indicating whether they are any entity identified on the Covered List, coupled with procedures for revocation for false statements or representations made in the application for certification, is a reasonable and cost-effective method to ensure that "covered" equipment is not certified. Because the attestation requirement is general, rather than a specific provision that directly relates to the equipment identified on the current Covered List, we believe that most applicants will rely on boilerplate language, that once incorporated for a single certification, will be of negligible cost for an applicant to include in future applications. We expect that our procedures for revocation for false statements or misrepresentations will deter most applicants from false attestations because of the cost that revocation would impose on an applicant. Moreover, we note that the attestation requirement that we are adopting is more cost effective than an alternative approach, such as a verification process whereby a third party would confirm that equipment being certified is not on the Covered List; that type of third party verification would be substantially more costly to applicants and would likely slow innovation. We believe that the costs we are imposing are reasonable in light of the national security goals.

---

[538] *Id.,* 36 FCC Rcd at 20698, para. 72.

[539] *See, e.g.*, CTA Comments at 22; CTA June 11, 2021 *Ex Parte* at 2; CTIA Comments at 2; TIA Comments at 11; Dahua USA Comments at 4; Dahua USA Jan. 4, 2022 *Ex Parte* at 13.

[540] *See, e.g.*, ENS Security Comments at 2; Huawei Technologies Comments at 15.

[541] Hikvision USA Reply Comments at 3.

[542] Hikvision USA Nov. 17, 2021 *Ex Parte* at 20-23; Hikvision USA Feb. 23, 2022 *Ex Parte* at 4-5.

[543] Dahua USA Reply Comments at 22-25.

[544] IPVM Comments at 4.

[545] Secure Equipment Act §§ 2(a)(2).

223. Similarly, we find that requiring that the each applicant for equipment certification designate a contact in the United States to act as an agent for service of process is reasonable and cost effective. No commenters raised concerns about the cost-effectiveness of this approach. As discussed above, the Commission has encountered difficulties in achieving service of process for enforcement matters involving foreign-based equipment manufacturers, and this helps ensure that the attestation requirement and other requirements associated with the prohibitions on "covered" equipment are enforceable.

224. *SDoC rules*. In light of the Commission's limited direct involvement in the SDoC process, we find that our rule prohibiting any of the entities (or their respective subsidiaries or affiliates) specified on the Covered List from using the SDoC process to authorize any equipment is a reasonable, cost-effective approach to safeguard national security. Because these entities or their subsidiaries or affiliates may produce "covered" equipment that poses an unacceptable risk to national security, even if these entities provide assurance that their equipment not included on the Covered List complies with appropriate technical standards, we cannot be confident that such equipment does not pose a risk to national security. Directing all equipment authorization applications produced by entities named on the Covered List through the certification process, coupled with our revisions to the SDoC attestation requirements, will allow appropriate scrutiny and oversight by the Commission to ensure consistent application of our prohibition on further equipment authorization of "covered" equipment.

225. We also conclude that adopting, as proposed, the requirement that all responsible parties seeking to utilize the SDoC process attest that the subject equipment is not produced by any entities (or their respective subsidiaries or affiliates) identified on the Covered List is a reasonable and cost-effective means of ensuring that any equipment produced by those entities, instead, is processed through the equipment certification process. We find this attestation requirement provides an appropriate means to ensuring that the SDoC process cannot be used to evade our restriction on use of the SDoC process (and instead require certification) with regard to entities that produce "covered" equipment.

226. The adopted rules associated with the SDoC process are narrowly tailored and a cost-effective means of achieving the Commission's overarching national security goals in this proceeding. They also are more cost-effective than other alternatives, such as changing the general rules by, for instance, requiring a registry or a central database specific to entities on the Covered List or setting up a novel verification process for such entities. Our existing certification rules and procedures already encompass such means of verification without creating the need to design a new system to mitigate national security risk. Because our prohibition applies to subsidiaries and affiliates, when combined with the attestation requirement for responsible parties it will incentivize domestic importers who serve as responsible parties to take the straightforward steps to ensure that equipment produced by entities that produce "covered" equipment are processed in a consistent fashion pursuant to the certification process. This will substantially reduce the cost of enforcing our prohibition on importation and marketing of equipment on the Covered List.

2. Constitutional claims

227. We are unpersuaded by certain constitutional objections raised by Huawei Cos., Hikvision USA, and Dahua USA.[546] Consequently, these arguments provide no basis for undercutting our decision to adopt new equipment authorization rules in this Report and Order.[547]

a. Bill of attainder

228. We reject the claims of Huawei Cos., Hikvision USA, and Dahua USA that denying equipment authorizations for equipment on the Covered List would represent an unconstitutional bill of attainder.[548] The Supreme Court has identified three elements of an unconstitutional bill of attainder: (1) "specification of the affected persons," (2) "punishment," and (3) "lack of a judicial trial."[549] We find the showings in the record regarding the first and second elements inadequate here.

229. As a threshold matter, we clarify the framing of our bill of attainder analysis in light of the different formulations of those arguments employed by commenters. Depending in part on whether commenters raised their bill of attainder concerns before or after the enactment of the Secure Equipment Act, those arguments focused variously on: section 889 of the 2019 NDAA (which provided one of the four triggers for inclusion on the Covered List under the Secure Networks Act);[550] the Secure Equipment Act (which directed the Commission to enact rules clarifying that it would not issue equipment authorizations for equipment on the Covered List published by the Commission under the Secure Networks Act);[551] or the new Commission rules themselves.[552]

230. Because it is the Secure Equipment Act that ultimately directs the Commission to enact rules yielding the results that are the focus of commenters' bill of attainder concerns, we frame our bill of attainder analysis in terms of that statute.[553] Nonetheless, we make clear that our analysis below provides

---

[546] Among other things, the Commission sought comment on whether the Commission should consider revoking any existing equipment authorizations of specific equipment that constitutes covered equipment. *See, e.g.*, *NPRM*, 36 FCC Rcd at 10611-13, paras. 80-89. Because we continue to evaluate the appropriate approach to such issues in the Further Notice rather than resolving them in this Report and Order, we need not, and do not, address objections premised on the Commission ultimately revoking or withdrawing equipment authorizations granted prior to the rules adopted here. *See, e.g.*, Dahua USA Comments at 18-19, 20-21 (raising retroactivity and due process concerns in that regard); Huawei Cos. Comments at 34-35, 37-38 (raising retroactivity and due process concerns in that regard); Hikvision USA Reply at 56-57 (raising takings concerns in that regard).

[547] We do not address in the Report and Order all of the constitutional claims raised because some of them address objections premised on the Commission ultimately revoking or withdrawing equipment authorizations granted prior to the rules adopted here. *See, e.g.*, Huawei Comments at 34-35, 37-38 (raising retroactivity and due process concerns in that regard); Dahua USA Comments at 18-19, 20-21 (raising retroactivity and due process concerns in that regard); Hikvision USA Reply at 56-57 (raising takings concerns in that regard). Those issues are discussed in the Further Notice of Proposed Rulemaking when seeking comment on revocation of existing equipment authorizations.

[548] *See, e.g.*, Huawei Cos. Comments at 36; Hikvision USA Comments at 35 n.77; Hikvision USA Reply at 55; Hikvision USA Nov. 17, 2021 *Ex Parte* at 10-16; Dahua USA Comments at 17-18.

[549] *Selective Serv. Sys. v. Minn. Pub. Interest Research Grp.*, 468 U.S. 841, 847 (1984).

[550] *See, e.g.*, Hikvision USA Comments at 35 n.77.

[551] *See, e.g.*, Hikvision USA Nov. 17, 2021 *Ex Parte* at 10-11.

[552] *See, e.g.*, Dahua USA Comments at 17-18; Huawei Cos. Comments at 36.

[553] Building on a foundation of several laws that came before it, the Secure Equipment Act directed the Commission to "clarify that the Commission will no longer review or approve any application for equipment authorization for equipment that is on the list of covered communications equipment or services published by the Commission under section 2(a) of the" Secure Networks Act. Secure Equipment Act § 2(a)(2).

sufficient grounds to reject commenters' bill of attainder arguments however they are framed or viewed.[554]

231. We reject claims that the Secure Equipment Act is an unconstitutional bill of attainder for a number of independent reasons. For one, it is not clear that the constitutional prohibition on bills of attainder protects corporations, as opposed to individuals.[555] To the extent that it does not protect corporations, its protections would be unavailable to the commenters that raised bill of attainder concerns here. Even if the constitutional prohibition on bills of attainder does protect corporations, however, courts have recognized that "it is obvious that there are differences between a corporation and an individual under the law," and as a result "any analogy between prior [bill of attainder] cases that have involved individuals and [cases] involv[ing] a corporation, must necessarily take into account this difference."[556] At a minimum, then, the distinction between corporations and individuals informs our analysis below.

232. *The "specification" criteria*. In significant part, the Secure Equipment Act also does not involve a specification of the affected persons as necessary to constitute a bill of attainder. Although initial iterations of the Covered List – identifying the equipment, products, and services of certain specified companies – had been published by the time the Secure Equipment Act was enacted, the Covered List required by the Secure Networks Act was designed to evolve over time, expanding or contracting based on the four statutory triggers for inclusion on that list.[557] Thus, we are not persuaded that the specificity prong would be satisfied by the existence of the Covered List at the time of the Secure Equipment Act's enactment.[558]

---

[554] In addition to the analysis below, insofar as the bill of attainder arguments are directed at Commission rules themselves, they fail to demonstrate that the Bill of Attainder Clause applies to agency regulations (rather than enacted legislation). *See, e.g.*, *In re FCC 11-161*, 753 F.3d 1015, 1088 (10th Cir. 2014) ("In this case [involving FCC rules], there has been no legislative act, let alone one that punishes Allband without a judicial trial. Consequently, Allband has failed to establish the existence of an unconstitutional Bill of Attainder." (footnote omitted)); *Scheerer v. U.S. Atty. Gen.*, 513 F.3d 1244, 1253 n.9 (11th Cir. 2008) ("We have never held that the Constitution's Bill of Attainder Clause, U.S. Const. art. I, § 9, cl. 3, is applicable to Executive Branch regulations, and other courts have suggested to the contrary."); *Glob. Relief Found., Inc. v. O'Neill*, 315 F.3d 748, 755 (7th Cir. 2002) ("Application of the IEEPA is not a bill of attainder; implementation of the statute is in the hands of the Executive and Judicial Branches, while a bill of attainder is a decision of guilt made by the Legislative Branch."); *In Paradissiotis v. Rubin*, 171 F.3d 983, 988 (5th Cir. 1999) ("No circuit court has yet held that the bill of attainder clause, U.S. Const. art. I, § 9, cl. 3, applies to regulations promulgated by an executive agency."). Insofar as the Clause does not apply to agency regulations, that is an additional, independent basis for rejecting the arguments directed at the Commission's rules themselves.

[555] *See, e.g.*, *Kaspersky Lab v. DHS*, 909 F.3d 446, 461 (D.C. Cir. 2018) (for purposes of that case "assum[ing] that the Bill of Attainder Clause protects corporations as well as natural persons"); *BellSouth Corp. v. FCC*, 162 F.3d 678, 684 (D.C. Cir. 1998) (*BellSouth II*) (noting that the parties had assumed that the Bill of Attainder clause protects corporations, and proceeding on that basis); *Huawei Tech. USA v. United States*, 440 F. Supp. 3d 607, 629 (E.D. Tex. 2020) (assuming without deciding that the Bill of Attainder clause protects corporations). *But see, e.g.*, *Consolidated Edison Co. of New York, Inc. v. Pataki*, 292 F.3d 338, 347 (2d Cir. 2002) (concluding that the Bill of Attainder clause protects corporations).

[556] *BellSouth II*, 162 F.3d at 684 (D.C. Cir. 1998); *see also, e.g.*, *Kaspersky*, 909 F.3d at 461 ("[A]lthough we assume that the Bill of Attainder Clause protects corporations as well as natural persons, we have no basis for likewise assuming that corporate entities feel burdens in the same way as living, breathing human beings." (citation omitted)); *ACORN v. United States*, 618 F.3d 125, 137 (2d Cir. 2010) ("'There may well be actions that would be considered punitive if taken against an individual, but not if taken against a corporation.'"); *Consolidated Edison Co.*, 292 F.3d at 354 ("Whether a government action is punishment varies depending on context. There may well be actions that would be considered punitive if taken against an individual, but not if taken against a corporation.").

[557] Secure Networks Act § 2(d).

[558] *See, e.g.*, *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 471-72 (1977) (the specificity criteria is not met by the Presidential Recordings and Materials Preservation Act, because although Title I referred to President Nixon by

(continued….)

233. Nor do most of the Secure Networks Act's triggers for inclusion on the Covered List represent a "specification" of affected persons for bill of attainder purposes. The first, second, and fourth triggers under the Secure Networks Act each turn on future "specific determination[s]" by relevant executive agencies and neither specifically identify companies or individuals by name, nor rely on a framework where the potentially-covered class ultimately subject to inclusion on the Covered List could be easily identified at the time the Secure Equipment Act was enacted. Nor do those triggers turn on past conduct defining the affected individual or group in terms of "irrevocable acts committed by them."[559] Consequently, we conclude that those triggers do not satisfy the "specification" prong of the bill of attainder analysis.[560] Admittedly, aspects of the trigger based on section 889(f)(3) of the 2019 NDAA do rely on certain classes of products and services from specifically-identified companies.[561] But the Secure Network Act's triggers do not otherwise identify the entities or individuals with products or services potentially subject to inclusion on the Covered List by name or in a manner that would render the covered class easily ascertainable when the Secure Equipment Act was enacted.[562]

---

name, Title II could apply to future presidents); *Hettinga v. United States*, 677 F.3d 471, 478 (D.C. Cir. 2012) ("'Since virtually all legislation operates by identifying the characteristics of the class benefited or burdened,' *BellSouth Corp. v. FCC*, 144 F.3d 58, 63 (D.C. Cir. 1998) (*BellSouth I*), the mere fact that the 'class' currently happens to contain only one member does not transform an open-ended statute into a bill of attainder." (citation modified)). Even assuming *arguendo* that the appearance on the covered list of equipment and services from certain named companies at the time of the Secure Equipment Act's enactment would satisfy the "specification" prong of the bill of attainder analysis for those companies as some claim, *see, e.g.*, Hikvision Nov. 17, 2021, *Ex Parte* Letter at 11, that would not provide grounds for such a finding regarding the operation of the Secure Equipment Act more generally.

[559] *Selective Serv.*, 468 U.S. at 848.

[560] The Secure Networks Act's triggers potentially fall outside the Bill of Attainder Clause for a further reason, depending on the details of how they are implemented in particular instances. "The [Bill of Attainder] Clause is concerned with punishment of individuals, not objects." *SeaRiver Maritime Fin. Holdings v. Mineta*, 309 F.3d 662, 672 (9th Cir. 2002) (citing *Fresno Rifle & Pistol Club, Inc. v. Van De Kamp*, 965 F.2d 723, 728 (9th Cir.1992) as "clarifying that a statute restricting the use of assault weapons and listing those weapons by the manufacturer's name specified punishment based not only on the manufacturer's identity, but on 'particular firearms which it has found are particularly dangerous,' and holding that the statute was not an attainder" and *Cummings v. Missouri*, 71 U.S. (4 Wall.) 277, 320 (1866), described as "striking down a statute when it 'was intended to reach the person, not the calling'"). To the extent that the triggers lead to the inclusion of what is, properly understood, merely "equipment" on the Covered List, rather than individuals or companies, that would fall outside the purview of the Bill of Attainder Clause.

[561] *See Huawei Tech. USA*, 440 F. Supp. 3d at 629-30 ("Huawei argues that Section 889 meets the specificity requirement as it is mentioned by name in the statute. The Government 'do[es] not dispute that the specificity element is satisfied here[.]' The Court agrees that the specificity prong is clearly met in this case as Huawei, along with ZTE, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company, are mentioned by name in Section 889." (citation omitted)); *cf. Kaspersky*, 909 F.3d at 454 ("the government concedes, as it must, that section 1634 [of the 2018 NDAA] applies with specificity to Kaspersky").

[562] *See, e.g.*, *Nixon*., 433 U.S. 538 (the "specification" criteria is met where a statute applies "either to named individuals or to easily ascertainable members of a group"). Consequently, even if a court were to disagree with our analysis below that the Secure Equipment Act does not impose "punishment" for Bill of Attainder Clause purposes, the requirements of the Secure Equipment Act, and the implementing Commission rules, would be unaffected as it relates to these triggers for inclusion on the Covered List. In particular, the Secure Networks Act provides that "[i]f any provision of [the Secure Networks] Act, or the application of such a provision to any person or circumstance, is held to be unconstitutional, the remaining provisions of this Act, and the application of such provisions to any person or circumstance, shall not be affected thereby." Secure Networks Act § 10. The Secure Equipment Act relies on the Secure Networks Act's Covered List to identify the equipment for which the Commission must not issue equipment authorizations. In each instance where the Commission would refuse to issue equipment authorizations in accordance with the rules required by the Secure Equipment Act, we thus interpret the Secure

(continued….)

234. Aspects of the section 889-based trigger also do not appear to satisfy the "specification" criteria. For example, in addition to applying to certain classes of equipment and services from specifically-identified companies, section 889(f)(3) of the 2019 NDAA also covers "[t]elecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country."[563] Whatever individual companies might know or suspect about themselves, we are not persuaded that the class of companies potentially covered by that criteria would have been easily ascertainable to Congress at the time of the Secure Equipment Act's enactment. Nor are we persuaded that ownership by, or connection with, the Chinese government, even if existing at a given point in time, are irrevocable acts that could not be altered in the future thereby affecting whether given companies were potentially implicated by that trigger.

235. *The "punishment" criteria*. Even to the extent that the Secure Equipment Act meets the "specification" prong, we are not persuaded that the denial of equipment certification represents a "punishment" under bill of attainder clause precedent. A "punishment," in this context, is not merely a burden.[564] To determine whether a statute imposes punishment for purposes of the bill of attainder clause, courts look to: "(1) whether the challenged statute falls within the historical meaning of legislative punishment; (2) whether the statute, viewed in terms of the type and severity of burdens imposed, reasonably can be said to further nonpunitive legislative purposes; and (3) whether the legislative record evinces a congressional intent to punish."[565] While courts weigh these factors together, "the second factor – the so-called 'functional test' – invariably appears to be the most important."[566] Even where a statute imposes a sanction falling within the historical meaning of punishment under the first factor, it is not a bill of attainder if it "reasonably can be said to further nonpunitive legislative purposes" under the second factor and the legislative record does not contain "'smoking gun' evidence of punitive intent" under the third.[567]

236. The party challenging a statute on attainder grounds bears the burden to "establish that the legislature's action constituted punishment and not merely the legitimate regulation of conduct."[568] And because statutes are "presumed constitutional,"[569] "only the clearest proof [will] suffice" to invalidate a statute as a bill of attainder.[570] The record here falls far short of the required showing.

237. With respect to the historical test regarding punishment, Hikvision USA and Dahua USA contend that denial of equipment authorization for equipment on the Covered List resembles "an

---

Equipment Act (and the implementing Commission rules) to be applying the relevant trigger(s) in the Secure Networks Act in a particular circumstance within the meaning of the severability provision in section 10 of the Secure Networks Act. This reflects the reasonable understanding that, given the security and safety interests at stake, Congress would want as many of its requirements to continue to have force as possible in the event that a court would find some subset of them invalid.

[563] 2019 NDAA § 899(f)(3)(d).

[564] *See Selective Serv*., 468 U.S. at 851 ("That burdens are placed on citizens by federal authority does not make those burdens punishment.").

[565] *Selective Serv*., 468 U.S. at 852.

[566] *Kaspersky*, 909 F.3d at 455.

[567] *SBC Commc'ns v. FCC*, 154 F.3d 226, 242-43 (5th Cir. 1998).

[568] *Nixon*, 433 U.S. at 476 n.40.

[569] *Heller v. Doe by Doe*, 509 U.S. 312, 320 (1993).

[570] *Communist Party of U.S. v. Subversive Activities Control Bd*., 367 U.S. 1, 83 (1961).

employment bar, banishment, and a badge of infamy."[571] We find these comparisons unpersuasive. For one, "[b]ecause human beings and corporate entities are so dissimilar," any analogy between the acts at issue in the employment bar cases and the restriction on equipment authorization under the Secure Equipment Act is "strained at best."[572] That distinction is important given the rationales underlying prior employment bar decisions. The Supreme Court extended "punishment" to include employment bars, in part, because the restrictions at issue "violated the fundamental guarantees of political and religious freedom."[573] The record does not reveal such concerns here.[574]

238. While there is some retrospective aspect of section 889 – namely, that there needed to be a basis to create the terms of the statute – that is common. Generally, all statutes have prospective and retrospective bases. But the focus of punishment in the bill of attainder context is a determination of past wrongdoing and sanctioning that conduct. That is what is missing from section 889 and that is what distinguishes section 889 from functionally appearing punitive. Thus, the fact that section 889 does not serve as a trial-like adjudication with a retrospective focus supports the Government's assertion that section 889 is a nonpunitive statute. But the analysis does not end here."[575]

239. Rather than representing something akin to an employment bar, we find the limitations much more analogous to line-of-business restrictions, which precedent commonly does not treat as imposing a punishment.[576] Companies with equipment on the covered list remain free to manufacture, import, and market equipment that does not require equipment authorization from the Commission, for example, and the Secure Equipment Act also does not prohibit companies' business activities not

---

[571] Hikvision USA Nov. 17, 2021 *Ex Parte* at 14; *see also, e.g.*, *id*. at 14-15 (elaborating on those claims); Dahua USA Comments at 17-18 (analogizing the restrictions to being blacklisted);

[572] *Kaspersky*, 909 F.3d at 462.

[573] *BellSouth II*, 162 F.3d at 686.

[574] *See Kaspersky Lab, Inc. v. DHS*, 311 F. Supp. 3d 187, 208 (D.D.C. 2018), *aff'd*, 909 F.3d 446 (D.C. Cir. 2018) ("A statute that does not apply to any individual but instead deprives a large multinational corporation of one of its many sources of revenue does not threaten anyone's personal rights or freedoms."). Also in contrast to the employment bar precedent, inclusion of a company's equipment on the Covered List, and the associated limitation on Commission-issued equipment authorizations, does not constitute, and is not based on, any trial-like adjudication that the companies are guilty of past wrongdoing. *See, e.g.*, *De Veau v. Braisted*, 363 U.S. 144, 160 (1960) ("The distinguishing feature of a bill of attainder is the substitution of a legislative for a judicial determination of guilt."); *Fresno Rifle*, 965 F.2d at 727 (rejecting gun manufacturers' argument that "the legislature tried them and found their products to be 'assault weapons"' where California legislature made findings including that the named plaintiffs' firearms constituted "assault weapons"); *cf. Huawei Tech. USA*, 440 F. Supp. 3d at 638 ("[T]he focus of punishment in the bill of attainder context is a determination of past wrongdoing and sanctioning that conduct. That is what is missing from Section 889 [of the 2019 NDAA] and that is what distinguishes Section 889 from functionally appearing punitive. Thus, the fact that Section 889 does not serve as a trial-like adjudication with a retrospective focus supports the Government's assertion that Section 889 is a nonpunitive statute.").

[575] *Huawei Tech. USA v. United States*, 440 F. Supp. 3d 607, 638 (E.D. Tex. 2020).

[576] *See, e.g.*, *Kaspersky*, 909 F.3d at 463 ("the Bill of Attainder Clause tolerates statutes that, in pursuit of legitimate goals such as public safety or economic regulation, prevent companies from engaging in particular kinds of business or particular combinations of business endeavors"); *BellSouth II*, 162 F.3d at 686 (noting "that the Supreme Court has approved other line-of-business restrictions without ever suggesting that the restrictions constituted 'punishment,'" and citing *FCC v. National Citizens Committee for Broad*., 436 U.S. 775 (1978) as "upholding FCC rules banning broadcast licensee from owning newspaper in same market: and *Board of Governors of Fed. Reserve Sys. v. Agnew*, 329 U.S. 441 (1947) as "upholding conflict-of-interest statute that prevented employees of securities underwriting firms from simultaneously working for banks that belong to Federal Reserve System" and rejecting claims that a telecommunications service line-of-business restriction imposed on certain named companies was a bill of attainder); *SBC Commc'ns*, 154 F.3d at 232 (rejecting a bill of attainder challenge to line-of-business restrictions that precluded named operating companies from providing certain telecommunications equipment and services); *BellSouth I*, 144 F.3d at 65 (the Supreme Court "strongly suggested [in *United States v. Brown*, 381 U.S. 437(1965)] that line-of-business restrictions pose no bill of attainder concerns").

involving the United States. Thus, unlike the statutes at issue in the employment bar cases, the Secure Equipment Act does not prevent companies with equipment on the Covered List from engaging in their chosen businesses in those respects.[577]

240. We also reject claims that the limitations on Commission-issued equipment authorizations resemble banishment. Banishment, or exile, is the "[c]ompelled removal or banishment from one's native country."[578] It has "traditionally been associated with deprivation of citizenship, and does more than merely restrict one's freedom to go or remain where others have the right to be: it often works a destruction of one's social, cultural, and political existence."[579] Claims of banishment therefore typically arise in cases involving denaturalization, denationalization, and deportation proceedings.[580] In light of this context, it is questionable whether banishment applies to corporations at all.[581] Alternatively, even if banishment does apply to corporations, the Secure Equipment Act does not "banish" from the United States those companies with equipment on the Covered List. The statute does not destroy those companies' social, cultural, or political existence in this country.[582] And it does not remove those companies from the United States (or any subdivision thereof), nor does it restrict their ability to manufacture, import, and market equipment in the United States that is not included on the Covered List.

241. The distinction between corporations and individuals also is important because "the stain of a brand of infamy or disloyalty," characteristic of bills of attainder, matters to individuals in a way that it does not to corporations.[583] Unlike "flesh-and-blood humans . . . who, most likely, have but one country of citizenship," as well as "neighbors and colleagues and communities in whose good graces they hope to remain," corporate reputation "is an asset that companies cultivate, manage, and monetize."[584] "It is not a

[577] *See, e.g.*, *Kaspersky*, 909 F.3d at 462 ("all of the Supreme Court's employment ban cases have involved a legislative enactment barring designated individuals or groups from participation in specified employments or vocations"). Even insofar as the limitation on Commission-granted equipment authorizations could apply indefinitely, that does not alter our view. *See, e.g.*, *SBC Commc'ns*, 154 F.3d at 238 (citing *Hawker v. New York*, 170 U.S. 189, 196 (1898) (upholding indefinite prohibition of convicted felons from practicing medicine where the state was "not seeking to further punish a criminal, but only to protect its citizens from physicians of bad character"); *id*. at 242 (citing *BellSouth I*, 144 F.3d at 65 ("Even measures historically associated with punishment – such as *permanent* exclusion from an occupation – have been otherwise regarded when the nonpunitive aims of an apparently prophylactic measure have seemed sufficiently clear and convincing.") (emphasis added); *Dehainaut v. Pena*, 32 F.3d 1066, 1071 (7th Cir. 1994) ("Even where a fixed identifiable group . . . is singled out and a burden traditionally associated with punishment—such as permanent exclusion from an occupation—is imposed, the enactment may pass scrutiny under bill of attainder analysis if it seeks to achieve legitimate and non-punitive ends and was not clearly the product of punitive intent.") (same)). And, of course, there also always remains the possibility of Congress changing the law. *See, e.g.*, *ACORN*, 618 F.3d at 140 ("[W]e reject the plaintiffs' argument that the appropriations laws are punitive because they disqualify ACORN from federal funds even if the GAO investigation results in a favorable disposition for ACORN. Although there is no provision in the appropriations laws that ties the GAO investigation with ACORN's status to receive federal funds, Congress could, of course, modify the appropriations law following the GAO's investigation.").

[578] Black's Law Dictionary (10th ed. 2014).

[579] *SeaRiver*, 309 F.3d at 673.

[580] *See Poodry v. Tonawanda Band of Seneca Indians*, 85 F.3d 874, 902 (2d Cir. 1996).

[581] *See SeaRiver*, 309 F.3d at 673 (seeming to assume so but noting that banishment typically "refers to individuals").

[582] *See, e.g.*, *Huawei Tech. USA*, 440 F. Supp. 3d at 635 (recognizing that "'[b]anishment has traditionally been associated with deprivation of citizenship and 'does more than merely restrict one's freedom to go or remain where others have the right to be: it often works a destruction of one's social, cultural, and political existence,'" quoting *SeaRiver Mar. Fin. Holdings, Inc. v. Mineta*, 309 F.3d 662, 673 (9th Cir. 2002) (in turn quoting *Poodry v. Tonawanda Band of Seneca Indians*, 85 F.3d 874, 897 (2d Cir. 1996))).

[583] *Kaspersky*, 909 F.3d at 461.

[584] *Id.*

quality integral to a company's emotional well-being, and its diminution exacts no psychological cost."[585] Because corporations do not "feel burdens in the same way as living, breathing human beings,"[586] the bill of attainder analysis does not apply to them in the same way.[587] We thus reject claims that the limitation on Commission equipment authorizations resembles a badge of infamy.

242. The functional test regarding punishment also persuades us that limitations on Commission-issued equipment authorizations as required by the Secure Equipment Act furthers nonpunitive legislative purposes, and thus is not punishment for bill of attainder purposes. The functional test asks "whether the statute, viewed in terms of the type and severity of burdens imposed, reasonably can be said to further nonpunitive legislative purposes."[588] "It is not the severity of a statutory burden in absolute terms that demonstrates punitiveness so much as the magnitude of the burden relative to the purported nonpunitive purposes of the statute."[589]

243. The Secure Equipment Act includes a prospective focus, prohibiting the future Commission authorization of those products and thereby preventing their use in U.S. communications networks because the covered communications equipment is understood, under triggers established by Congress, as "pos[ing] an unacceptable risk to the national security of the United States or the security and safety of United States persons."[590] By restricting the Commission from authorizing such equipment going forward, the Secure Equipment Act seeks to guard against future risks "to the national security of the United States or the security and safety of United States persons" that would arise if the equipment on the Covered List could be used by communications providers and customers, rather than punishing companies with equipment on the Covered List for past conduct.[591] Thus, Congress ensured that the Commission could place equipment produced by any entity on the Covered List "if and only if," among

---

[585] *Id.*

[586] *Id.*

[587] *See id.*; *see also ACORN*, 618 F.3d at 137 (recognizing same); *Huawei Tech. USA*, 440 F. Supp. 3d at 631 (discussing *Kaspersky* and concluding that "this historical punishment applies to corporations in a different sense than it does to individuals"). Indeed, any reputational harm to a company as alleged here pales in comparison to the "costly injury to [the plaintiff]'s reputation" in *Foretich v. United States*, 351 F.3d 1198, 1223 (D.C. Cir. 2003), cited by Hikvision. *See* Hikvision Nov. 17, 2021, *Ex Parte* Letter at 15 n.71. In *Foretich*, the statute at issue "memorialize[d] a judgment by . . . Congress that [the plaintiff] [wa]s guilty of horrific crimes," namely "criminal acts of child sexual abuse" against his own daughter. *Foretich*, 351 F.3d at 1223.

[588] *SBC Commc'ns*, 154 F.3d at 242.

[589] *Foretich*, 351 F.3d at 1222.

[590] Secure Networks Act § 2(b)(1). In light of the enactment of the Secure Equipment Act, which directs the adoption of rules to "clarify that the Commission will no longer review or approve any application for equipment authorization for equipment that is on the" Covered List, Secure Equipment Act § 2(a)(2), we reject arguments that "there is absolutely no logical nexus between the Covered List and the proposed rules." Huawei Comments at 36. To the extent that commenters seek to define the nonpunitive interest being pursued here more narrowly by drawing from snippets of legislative history or past statements by individual Commissioners, *see, e.g.*, Hikvision Nov. 17, 2021, *Ex Parte* Letter at 12, we are not persuaded that Congress' objectives should be narrowed relative to what is stated in the relevant statutes themselves. *Cf.* H.R. Rep. No. 117-148, at 2 (Oct. 19, 2021) ("While the Secure and Trusted Communications Networks Act took important steps to remove compromised equipment from American networks, the law did not cover equipment that is purchased using private funds (i.e., without the use of federal funds provided by the Commission) and poses a similar national security threat *as is conceived under the Act*." (emphasis added)).

[591] *See, e.g.*, *Kaspersky*, 909 F.3d at 457 (identifying "'a rather conventional response' to a security risk: remove the risk"). For example, by seeking to comprehensively address the risks from equipment understood to "pos[e] an unacceptable risk to the national security of the United States or the security and safety of United States persons," Secure Networks Act § 2(b)(1), the Secure Equipment Act can be seen as akin to permissible regulation of entities "in certain inherently conflicted positions," rather "than an impermissible [punishment] censuring or condemning any man or group of men for their personal conduct." *SBC Commc'ns*, 154 F.3d at 243.

other things, it has capabilities associated with specific prospective national security risks – *i.e.*, of routing or redirecting traffic or permitting visibility into user data or packets, or causing remote disruption of the network – or "otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons."[592]

244. The burdens imposed by the Secure Equipment Act are also sufficiently tailored to the statute's prophylactic purposes. The Supreme Court has warned that Congress must be given sufficient leeway in making policy decisions, lest the bill of attainder analysis "cripple the very process of legislating."[593] Congress is therefore not required to "precisely calibrate the burdens it imposes to . . . the threats it seeks to mitigate."[594] A statute does not fail the functional test unless it is "significantly overbroad," such that it "pil[es] on . . . additional, entirely unnecessary burden[s],"[595] or so underinclusive that it "seemingly burdens one among equals."[596] The standard is a high one because the inquiry remains whether the statute is so punitive that it "belies any purported nonpunitive goals."[597]

245. We are unpersuaded by claims that the inability to obtain a Commission-issued equipment authorization for equipment on the Covered List should be considered "punishment" on the theories that the prohibitions are overbroad in scope or that there are narrower, less burdensome alternatives that could have been employed.[598] This approach to bill of attainder review runs afoul of the Supreme Court's warning against "crippl[ing] the very process of legislating."[599] The Bill of Attainder Clause does not command such a result.[600] Precluding the Commission from granting authorizations for equipment on the Covered List has a clear nexus to the nonpunitive prophylactic purpose of guarding against risks "to the national security of the United States or the security and safety of United States persons" that would arise if the equipment on the Covered List could be used by communications providers and customers.[601]

246. Further, whether or not Congress or policymakers arguably have treated all the equipment on the Covered List in an identical manner in other contexts that have implicated security

---

[592] 47 U.S.C. § 1601(b)(2).

[593] *Nixon*, 433 U.S. at 470.

[594] *Kaspersky*, 909 F.3d at 460; *see also SBC Comm'ns*, 154 F.3d at 243 (upholding statute in the absence of "substantial doubt [about] the fit of [its] tailoring").

[595] *Kaspersky*, 909 F.3d at 455, 460.

[596] *Kaspersky*, 909 F.3d at 456.

[597] *Foretich*, 351 F.3d at 1222.

[598] *See, e.g.*, Hikvision USA Nov. 17, 2021 *Ex Parte* at 12-13.

[599] *Nixon*, 433 U.S. at 470.

[600] *See id*.

[601] To the extent that commenters express concern that restrictions on Commission-issued equipment authorizations will encompass equipment not properly included in the Covered List, *see, e.g.*, Hikvision Nov. 17, 2021, *Ex Parte* Letter at 10, those concerns properly are directed at the reasonableness of a given statutory interpretation and not on whether the Secure Equipment Act imposes a punishment. And to the extent that the equipment is properly included on the Covered List, objections to the breadth of the scope of the Secure Equipment Act would need to focus on Congress's interest in addressing the future risks from any use of equipment understood to present threats "to the national security of the United States or the security and safety of United States persons" that would arise if the equipment on the Covered List could be used by communications providers and customers, rather than focusing on more narrowly-defined categories of risks as conceived of by the commenters or others. *See, e.g.*, Hikvision Nov. 17, 2021, *Ex Parte* Letter at 12. Our interpretation of the scope of the Covered List as relevant here, and our understanding of the relevant security risks, are discussed more generally below. *See generally supra* Section III.B and III.C.

concerns does not demonstrate that treating them similarly in this context is punitive, as some allege.[602] This is particularly true insofar as Congress might continue to learn from its experiences as it legislates against the backdrop of prior actions in this area.[603] Under the applicable standard, "the question is not whether a burden is proportionate to the objective, but rather whether the burden is so disproportionate that it belies any purported nonpunitive goals."[604]

247. Nor are we persuaded by Hikvision USA's claim that Congress instead could have relied entirely on the framework used in the Federal Acquisition Supply Chain Security Act of 2018, under which "any company potentially subject to an exclusion or removal order would receive notice, including the relevant procedures and basis, a chance to respond, and an avenue for judicial review."[605] Determinations made under that framework are, in fact, one basis for inclusion in the Covered List,[606] but we are not persuaded that (or an analogous approach) needs to be the exclusive mechanism for identifying equipment presenting security risks that warrant triggering inclusion on the Covered List and the associated restriction on Commission equipment authorizations under the Secure Equipment Act. Given the wide latitude afforded Congress to choose between policy alternatives, it "does not matter that Congress arguably could have enacted different legislation in an effort to secure federal networks, because it cannot be legitimately suggested that the risks . . . were so feeble that no one could reasonably assert them except as a smoke screen for some invidious purpose."[607]

248. We also reject arguments that the Secure Equipment Act is underinclusive.[608] To the extent that these arguments proceed from the assumption the Covered List only includes a limited, finite set of equipment from specific companies, they neglect the fact that the Covered List is designed by Congress to be updated over time – including reversing prior determinations – as additional determinations are made regarding security risk. This fact underscores that the statute's purpose is to counter a persistent threat, not to punish a particular company.[609] Separately, the Supreme Court has

---

[602] *See, e.g.*, Hikvision USA Nov. 17, 2021 *Ex Parte* at 12-13.

[603] *See, e.g.*, *Kaspersky*, 909 F.3d at 456 (although "the functional test is 'more exacting' than rational basis review," "the Bill of Attainder Clause does not require narrow tailoring," and "Congress enjoys leeway to select among more or less burdensome options, and it 'may read the evidence before it in a different way than might this court or any other, so long as it remains clear that Congress was pursuing a legitimate nonpunitive purpose'"); *BellSouth I*, 144 F.3d at 66 (although prior understandings of the marketplace held by the Department of Justice and the D.C. Circuit in the past led them to conclude that certain regulatory measures were not needed, even the court's prior understanding "never suggested that the risks of anticompetitive conduct were so feeble that no one could reasonably assert them except as a smokescreen for some invidious purpose (much less for the specific invidious purpose of 'punishing' the BOCs)").

[604] *Kaspersky Lab*, 909 F.3d at 455.

[605] Hikvision USA Nov. 17, 2021 *Ex Parte* at 13 (citing Federal Acquisition Supply Chain Security Act of 2018, Pub. L. 115-390, Title II, 132 Stat. 5173, 5181–82 (2018)).

[606] Secure Networks Act § 2(c)(1) (establishing as a trigger: "[a] specific determination made by any executive branch interagency body with appropriate national security expertise, including the Federal Acquisition Security Council established under section 1322(a) of title 41, United States Code"). 41 U.S.C. § 1322(a) reflects the codification of section 1322(a) of Title II of the Federal Acquisition Supply Chain Security Act of 2018.

[607] *Kaspersky*, 909 F.3d at 459; *see also id*. ("The Bill of Attainder Clause does not make perfect the enemy of the good.").

[608] *See, e.g.*, Hikvision USA Nov. 17, 2021 *Ex Parte* at 13.

[609] *See Nixon*, 433 U.S. at 472; *Kaspersky*, 909 F.3d at 459-60 (noting significance of broader provision directing further study of the Russian cyber-threat and the possibility of Congress expanding the statute's prohibition to other companies); *Fresno Rifle*, 965 F.2d at 724 (where statute provided process for future designations of "assault weapons," purpose was not to punish the named manufacturers but to control types of weapons); *Huawei Tech. USA*, 440 F. Supp. 3d at 644 ("Notably, Section 889 [of the 2019 NDAA] leaves open the possibility of designating additional companies to be subject to the prohibitions identified in the statute based on the recommendation of the

(continued….)

explained that a law is not an unconstitutional attainder by virtue of its specificity, and there is no requirement that Congress pass only laws that are generally applicable.[610] Such a requirement would leave Congress powerless to address national security threats directly whenever the person or entity posing the threat is specifically identifiable. The courts have therefore roundly—and rightly—rejected such an irrational result.[611]

249. In addition, we are unpersuaded by Hikvision USA's claim that the Secure Equipment Act imposes punishment based on the Congressional motivations underlying its enactment.[612] The Supreme Court has cautioned that "[j]udicial inquir[y] into Congressional motives [is] at best a hazardous matter" and that "the presumption of constitutionality" that attaches to a congressional enactment "forbids . . . [a] reading of the statute's setting which will invalidate it over that which will save it."[613] Accordingly, "only the clearest proof" will render a statute unconstitutional based on congressional intent.[614] "[I]solated statements" do not suffice.[615] Yet commenters only muster isolated statements from individual legislators in support of their bill of attainder arguments here.[616] We find such arguments particularly unpersuasive against the backdrop of the extensive history of concerns about U.S. safety and security in light of the sorts of equipment that are, and can be, included on the Covered List, which makes manifest its nonpunitive prophylactic purpose.[617]

b. Equal protection

250. We reject Hikvision USA's arguments that our actions here violate constitutional requirements of equal protection.[618] In particular, we reject the claim that the new equipment authorization rules target certain companies "on the basis of national origin or alienage" and should be

DNI or the Director of the FBI. Congress's determination of the legitimate class of individual companies that posed the greatest threat and the ability to subsequently add companies that are determined to pose a threat supports the nonpunitive purposes asserted in this case.").

[610] *See, e.g.*, *Plaut v. Spendthrift Farm, Inc.*, 514 U.S. 211, 239 (1995) ("While legislatures usually act through laws of general applicability, that is by no means their only legitimate mode of action . . . . Even laws that impose a duty or liability upon a single individual or firm are not on that account invalid . . . ."); *Nixon v. Administrator of General Services*, 433 U.S. at 471 ("However expansive the prohibition against bills of attainder, it surely was not intended to serve as a variant of the equal protection doctrine, invalidating every Act of Congress or the States that legislatively burdens some persons or groups but not all other plausible individuals." (footnote omitted)).

[611] *See Bank Markazi v. Peterson*, 136 S. Ct. 1310, 1328 (2016) (citing cases).

[612] *See, e.g.*, Hikvision USA Nov. 17, 2021 *Ex Parte* at 15-16.

[613] *Flemming v. Nestor*, 363 U.S. 603, 617 (1960).

[614] *Flemming*, 363 U.S. at 617; *see also, e.g.*, *Communist Party of U.S. v. Subversive Activities Control Bd.*, 367 U.S. 1, 83 (1961) (If a law is challenged as a bill of attainder based on the motivation of Congress in enacting it, "only the clearest proof could suffice to establish the unconstitutionality of a statute on such a ground."); *SBC Commcn's*, 154 F.3d at 243 ("[W]e reason that the Special Provisions are not punitive because neither their terms nor their legislative history demonstrates the 'smoking gun' evidence of punitive intent necessary to establish a bill of attainder. As the Supreme Court clarified in Selective Service, ' 'unmistakable evidence of punitive intent ... is required before a Congressional enactment of this kind may be struck down' ' on attainder grounds.").

[615] *Selective Serv.*, 468 U.S. at 856; *see also SBC Commc'ns*, 154 F.3d at 243 (similar).

[616] *See, e.g.*, Hikvision USA Nov. 17, 2021 *Ex Parte* at 15-16. Even less relevant to this inquiry into legislative motivation are filings made by members of the general public in this proceeding or elsewhere that commenters allege reveal a punitive motivation on the part of the filers. *See, e.g.*, Hikvision USA Reply at 55.

[617] *See, e.g.*, *NPRM*, 36 FCC Rcd at 10580-89, paras. 6-22.

[618] *See, e.g.*, Hikvision USA Comments at 65-71; Hikvision USA Nov. 17, 2021 *Ex Parte* at 16.

subject to strict scrutiny under the equal protection clause.[619] The premise underlying the inclusion of companies on the Covered List is that "communications equipment or service, . . . produced or provided by such entity poses an unacceptable risk to the national security of the United States or the security and safety of United States persons."[620] Although some commenters premise their equal protection concerns on the theory that they are being targeted merely because they are Chinese,[621] we observe that status as a Chinese company—or even a relationship with the Chinese government—is not, standing alone, sufficient (or necessary) for inclusion on the Covered List.[622] Ownership by, or connection with, the Chinese government is only one element of one possible basis for inclusion on the covered list,[623] which also always critically depends on judgments about the technical characteristics and national security risks associated with the covered equipment and services.[624] Because the treatment of these companies, as properly understood, does not turn on any suspect classifications, nor does it infringe fundamental constitutional rights, it only is subject to rational basis scrutiny under equal protection precedent.[625] The

[619] Hikvision USA Comments at 66-67; *see also, e.g.*, Hikvision USA Comments at 68-70; Hikvision USA Nov. 17, 2021 *Ex Parte* at 16.

[620] Secure Networks Act § 2(b); *see also* Secure Equipment Act § 2(a)(2) (requiring that rules adopted in this proceeding "clarify that the Commission will no longer review or approve any application for equipment authorization for equipment that is on the list of covered communications equipment or services published by the Commission" on the Covered List under the Secure Networks Act).

[621] *See, e.g.*, Hikvision USA Comments at 66 ("The Commission targets Hikvision and other companies because they are "covered telecommunications equipment" manufacturers. And those companies are covered manufacturers for only one reason: they are Chinese." (footnote omitted)).

[622] As a result, this scenario is a far cry from cases like those cited by Hikvision finding actual or plausible equal protection violations where the government broadly targeted individuals of a given national origin or alienage for differential treatment. *See, e.g.*, Hikvision USA Comments at 67 (citing *Yick Wo v. Hopkins*, 118 U.S. 356 (1886) (San Francisco ordinance applied in practice just to restrict Chinese nationals) and *Takahashi v. Fish & Game Comm'n*, 334 U.S. 410 (1948) (restriction on commercial fishing licenses for anyone ineligible to become a U.S. citizen)); Hikvision USA Nov. 17, 2021 *Ex Parte* at 16 (citing *Adarand Constructors, Inc. v. Pena*, 515 U.S. 200 (1995) (federal government practice of giving general contractors financial incentives to hire socially and economically disadvantaged subcontractors, which presumptively was defined to include "Black Americans, Hispanic Americans, Native Americans, Asian Pacific Americans, and other minorities") and *NAACP v. U.S. Dep't of Homeland Sec.*, 364 F. Supp. 3d 568 (D. Md. 2019) (terminating Temporary Protected Status under immigration law for Haitian nationals).

[623] Even the consideration of ownership by, or connection with, the Chinese government as an element of the analysis comes against the backdrop of recognition that this bears on the associated national security risk. *See, e.g.*, *Supply Chain Order and Further Notice*, 34 FCC Rcd at 11425, paras. 6-7 (discussing a 2010 letter from members of Congress to the Commission and a 2012 report from the House Permanent Select Committee on Intelligence); *id.* at 11433, para. 27 (concluding that certain "companies' ties to the Chinese government and military apparatus – together with Chinese laws obligating them to cooperate with any request by the Chinese government to use or access their systems – pose a threat to the security of communications networks and the communications supply chain"); *id.* at 11440-42, paras. 44-46 (discussing security risks associated with a company's nexus with the Chinese government).

[624] Specifically, to be "covered," the Secure Networks Act provides that such equipment must meet two criteria. First, the communications equipment or service must, based exclusively on determinations made by Congress, certain government agencies, or interagency bodies, "pose[] an unacceptable risk to the national security of the United States or the security and safety of United States persons[.]" Secure Networks Act § 2(b)(1). Second, the equipment or services must be "capable of – (A) routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles; (B) causing the network of a provider of advanced communications service to be disrupted remotely; or (C) otherwise posing an unacceptable risk to the national security of the United States or the security and safety of United States persons." *See id.* § 2(a).

[625] *See, e.g.*, *FCC v. Beach Commc'ns*, 508 U.S. 307, 313 (1993) ("in areas of social and economic policy, a statutory classification that neither proceeds along suspect lines nor infringes fundamental constitutional rights must (continued….)

treatment of these companies under the new equipment authorization rules adopted here readily satisfies rational basis review for the same reasons the Commission finds the new rules warranted more generally.[626]

251. In the alternative, even assuming arguendo that strict scrutiny applied, we conclude that standard would be satisfied here.[627] Promoting national security is a compelling interest, as the Commission has recognized previously.[628] We also find our new rules narrowly tailored to advance that interest. Those rules target the specific equipment identified as posing "an unacceptable risk to the national security of the United States or the security and safety of United States persons" under the framework of the Secure Networks Act,[629] which involves either a judgment regarding national security risks made by Congress itself or through a specific executive branch analysis in that regard.[630] Congress further concluded in the Secure Equipment Act that, in order to address those security risks, it was necessary for the Commission to deny equipment authorization for the equipment on the Covered List.[631] Our analysis of our new rules more generally likewise affirms the need to take this step to guard against the national security risks associated with equipment on the Covered List.[632] Given that, we are unpersuaded by some commenters' claims that the rules are overinclusive.[633] We also do not find the rules underinclusive. Contrary to some commenters' claims, the Covered List and our associated equipment authorization rules do not narrowly focus on companies linked to the Chinese government to the exclusion of companies from other countries, which arguably present similar security risks.[634] While those comments myopically focus on the equipment actually included on the Covered List at a given moment in time, the Covered List is an evolving inventory of certain communications equipment and services found to present an unreasonable security risk under the Secure Networks Act's framework.[635]

---

be upheld against equal protection challenge if there is any reasonably conceivable state of facts that could provide a rational basis for the classification"); *City of Cleburne v. Cleburne Living Center*, 473 U.S. 432, 441-42 (1985) ("where individuals in the group affected by a law have distinguishing characteristics relevant to interests the State has the authority to implement, the courts have been very reluctant, as they should be in our federal system and with our respect for the separation of powers, to closely scrutinize legislative choices as to whether, how, and to what extent those interests should be pursued"); *see also*, *e.g.*, *Mathews v. Diaz*, 426 U.S. 67, 82-84 (1976) (applying rational basis review and upholding a federal law limiting Medicare benefits to some aliens but not others).

[626] *See generally supra* Section III.B, C.

[627] *See, e.g.*, *Adarand*, 515 U.S. at 227 (strict scrutiny requires that legal requirements be "narrowly tailored measures that further compelling governmental interests").

[628] *See, e.g.*, *Supply Chain 2nd R&O*, 35 FCC Rcd at 14329, para. 103 (noting "the compelling national security interests to promptly remove insecure equipment and services from our networks"); *China Unicom (Americas) Operations Limited*, Order on Revocation, FCC 22-9, para. 47 n.195 (Feb. 2, 2022) (*China Unicom Revocation Order*) (citing, among other things, *Haig v. Agee*, 453 U.S. 280, 307 (1981) ("It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation."")). Even Hikvision concedes that "promoting national security – the Commission's stated goal here – can be a compelling interest." Hikvision USA Comments at 67.

[629] Secure Networks Act § 2(b).

[630] *Id.* § 2(b)(1), (c).

[631] *Id.* § 2(a).

[632] *See generally supra* Section III.B, C.

[633] *See, e.g.*, Hikvision USA Comments at 68-69.

[634] *See, e.g.*, *id.*

[635] Indeed, although no new communications equipment has been added to the Covered List yet, subsequent executive branch determinations have triggered the addition of new products and services to the Covered List. *March 2022 Covered List Public Notice* (adding Kaspersky-branded products and China Telecom's services

(continued….)

We expect that evidence of national security risks associated with other communications equipment and services similar to that posed by the equipment and services already on the Covered List likewise would lead to determinations under the review frameworks that would trigger inclusion of those equipment and services on the Covered List, and we see no basis in the record to suppose otherwise.

c. Takings

252. Nor are we persuaded by Hikvision USA that the rules we adopt here represent a taking of property in violation of the Fifth Amendment.[636] For one, we find that our rules do not represent a *per se* taking. Our rules do not appropriate the equipment at issue for government use,[637] nor are we persuaded that our rules deny owners of the relevant equipment "*all* economically beneficial us[e]" of their property,[638] given that the lack of Commission equipment authorization does not preclude it from, among other things, marketing, selling, or using the equipment outside the U.S.

253. We also reject assertions that our rules represent a regulatory taking. The principal factors a court will review in determining whether a governmental regulation effects a taking are: (a) the character of the governmental action; (b) the economic impact of that action; and (c) the action's interference, if any, with investment-backed- expectations.[639] Regarding the first factor, as noted above the rules adopted here do not appropriate the relevant equipment for government use, but instead promotes a significant common good by promoting national security and protecting the nation's communications infrastructure from potential security threats.[640] With respect to the second factor, even assuming *arguendo* some diminution in value of the equipment actually addressed by the Commission's actions in this Report and Order – *i.e.*, equipment that has not yet received Commission authorization, that is merely necessary – but not sufficient – to demonstrate a regulatory taking.[641] Nor are we persuaded

---

associated with its section 214 authorizations); *September 2022 Covered List Public Notice* (adding PacNet/ComNet and China Unicom services).

[636] Hikvision USA Reply at 56-57. It is not clear that Hikvision actually seeks to raise takings claims outside the specific scenario where the Commission were to revoke or withdraw preexisting equipment authorizations. Out of an abundance of caution we consider such a theory in a manner commensurate with Hikvision's ambiguous, minimal explication in that regard, and ultimately find any such claims unpersuasive.

[637] *See, e.g.*, *Horne v. Dep't. of Agric.*, 576 U.S. 350, 359-61 (2015) (*per se* takings implicated when the government appropriates real or personal property for its own use).

[638] *Lucas v. S.C. Coastal Council*, 505 U.S. 1003, 1019 (1992).

[639] *Penn Central Transp. Co. v. New York City*, 438 U.S. 104, 124 (1978).

[640] *See, e.g.*, *China Unicom Revocation Order*, FCC 22-9, para. 47 (even assuming *arguendo* there was a property interest at stake there, concluding with respect to the first *Penn Central* factor that "revoking CUA's section 214 authority clearly furthers the public interest, convenience, and necessity because it promotes a significant common good: ensuring national security and protecting the nation's communications infrastructure from potential security threats"); *Penn Central*, 438 U.S. at 124 (holding as to the first factor that a taking "may more readily be found when the interference with property can be characterized as a physical invasion by government . . . than when interference arises from some public program adjusting the benefits and burdens of economic life to promote the common good." (citation omitted)).

[641] *See, e.g.*, *Concrete Pipe & Prods., Inc. v. Constr. Laborers Pension Trust*, 508 U.S. 602, 645 (1993) (Supreme Court precedent has "long established that mere diminution in the value of property, however serious, is insufficient to demonstrate a taking."); *A&D Auto Sales, Inc. v. United States*, 748 F.3d 1142, 1157 (Fed. Cir. 2014) ("In order to establish a regulatory taking, a plaintiff must show that his property suffered a diminution in value or a deprivation of economically beneficial use. . . . '[I]f the regulatory action is not shown to have had a negative economic impact on the [plaintiff's] property, there is no regulatory taking.'"). Hikvision cites *Andrus v. Allard*, 444 U.S. 51 (1971), and claims that, in contrast to the rights that remained in that case—where no takings was found—the "the Commission's rules would deny manufacturers virtually all of their rights in covered products." Hikvision Reply at 57. As noted above, however, the equipment at issue here still could be, among other things, marketed, sold, and used outside the U.S., and it is not clear why that is materially different from the Court's acknowledgment (continued….)

that our rules interfere with reasonable investment-backed expectations under the third factor. The equipment at issue has long been subject to Commission authorization requirements, and the Supreme Court has recognized that for property that has "had long been subject to federal regulation" there was no "reasonable basis to expect" that the regulatory regime would not change.[642] Indeed, the reasonableness of any expectations regarding the not-yet-authorized equipment addressed by this Report and Order is especially doubtful, given the years of legislative and regulatory focus on possible security-related restrictions on such equipment.[643] Particularly in light of "the heavy burden placed upon one alleging a regulatory taking,"[644] we find no basis to find a regulatory taking on the record here.

d. Separation of powers

254. We also are unpersuaded by Hikvision that Commission actions would be invalid on separation of powers grounds.[645] In particular, Hikvision contends that "[b]ecause the FCC Commissioners are appointed by the President and wield significant powers that are executive in nature, but are not removable at will by the President, their status may well conflict with the Constitution's separation of powers" in the event that certain recent Supreme Court precedent regarding Presidential removal were "to be applied to multi-member agencies like the FCC."[646] But insofar as the Supreme Court has not gone that far – as Hikvision itself observes – we are not persuaded to find constitutional concerns in that regard ourselves.[647]

3. WTO and Mutual Recognition Agreements

255. *World Trade Organization (WTO).* In its comments, the People's Republic of China (PRC) argues that placing only Chinese companies on the Covered List violates non-discriminatory principles in the World Trade Organization/Technical Barriers to Trade (WTO/TBT) agreement.[648] In particular, it asserts article 2.1 of that agreement requires that member countries ensure that, in their technical regulations, products imported from other members must be accorded no less favorable

---

of the continued practical and economic use of the property at issue in *Andrus v. Allard*. *See, e.g.*, *Andrus v. Allard*, 444 U.S. at 66 ("that appellees retain the rights to possess and transport their property, and to donate or devise the protected birds"); *id*. ("[i]n the instant case, it is not clear that appellees will be unable to derive economic benefit from the artifacts; for example, they might exhibit the artifacts for an admissions charge"). And as *Andrus v. Allard* also observes, "perhaps because of its very uncertainty, the interest in anticipated gains has traditionally been viewed as less compelling than other property-related interests." *Id*.

[642] *Concrete Pipe & Prods.*, 508 U.S. at 645-46.

[643] Particularly since the mid-2010s, concern about network equipment and security has been evident in federal statutes, executive orders, and Commission regulatory actions. *See, e.g.*, *NPRM*, 36 FCC Rcd at 10579-89, paras. 5-22 (discussing statutes, executive orders, and Commission regulatory consideration of network equipment and security).

[644] *Keystone Bituminous Coal Ass'n v. DeBenedictis*, 480 U.S. 470, 493 (1987).

[645] Hikvision USA Comments at 71-72.

[646] *Id.*

[647] Separately, even assuming *arguendo* that a court were to decide in the future that for-cause removal protections for FCC Commissioners were unconstitutional, the record does not provide any reason to presume that the court would invalidate Commission action on that basis. The Communications Act does not expressly provide for-cause removal protections for Commissioners, and the record does not provide a basis to assume that the hypothetical court would invalidate Commission action rather than instead simply declining to infer the existence of what that court would see as unconstitutional for-cause removal protections.

[648] People's Republic of China Comments at 3. These comments were submitted by MaryAnn Hogan on behalf of Zhao Minggang, Deputy Director General, China World Trade Organization/Technical Barriers to Trade (WTO/TBT)).

treatment,[649] and that prohibiting the authorization of equipment and services on the Covered List violates WTO/TBT transparency principles in the absence of a public technical standard and measurement index.[650] Similar concerns are raised by Dahua, which urges the Commission to consider whether its proposed rule may implicate U.S. obligations through the WTO or the General Agreement on Tariffs and Trade.[651]

256. We find that, contrary to those assertions, our actions here are consistent with the United States' international obligations under the WTO/TBT agreement. As discussed above and clearly laid out in statute, the Commission is required to include on the Covered List equipment and services based solely on determinations by four enumerated U.S. Government sources relating to national security. Under the relevant statutes, those determinations are not made, as suggested by these commenters, on the basis of nationality but are made based on fact-specific reviews whether the relevant equipment and services are found to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons, and not on sweeping determinations on the basis of nationality. Indeed, the March 2022 update to the Covered List includes equipment and services from countries other than China.[652] Finally, we note that nearly all products from China will remain eligible for equipment authorization under our new rules. Therefore, we find that the commenters' concerns are without merit.

257. *Potential Impact on Global Trade and Mutual Recognition Agreements.* Noting the "robust" international trade in consumer electronics, CTA asks that the Commission consider how changes to its equipment authorization program would impact relationships and policies with global trade partners, including possible retaliatory actions by China.[653] In particular, CTA asks that the Commission consider potential impacts on the mutual recognition agreements (MRAs) that expedite trade, including the recognitions that participating countries give to each other's testing labs and certification bodies in order to speed time to market and decrease regulatory costs to manufacturers.[654] Dahua also requests that the Commission consider whether adoption of its proposed rules could cause China to take retaliatory trade action.[655]

258. We have considered whether the proposed rules would have impacts on our relationships with our global trade partners, and in particular on MRAs. MRAs are expressly designed with recognition that equipment authorization processes are continually evolving. MRAs establish a process for the recognition of conformity assessment bodies and the acceptance of conformity assessment results without fixing the precise requirements to which products must conform, as these requirements evolve over time. They also typically include clauses on the preservation of regulatory authority in recognition of the need for future updates to such requirements. The changes to our rules adopted in this Report and Order merely update the requirements for authorizing equipment, without affecting which conformity

[649] *Id.* ("In accordance with Article 2.1 of the TBT Agreement, Members shall ensure that in respect of technical regulations, products imported from the territory of any Member shall be accorded treatment no less favourable than that accorded to like products of national origin and to like products originating in any other country. . .").

[650] *Id.* ("Without a public technical standard and measurement index, the fact that the United States deems products of Chinese enterprise to have security threats is violating the WTO/TBT transparency principles. …").

[651] Dahua USA Reply Comments at 25.

[652] On March 25, 2022, PSHSB updated the Covered List to include Kaspersky-branded products, based on new determination by the Department of Homeland Security, and China Telecom and China Mobile International USA services, based on new determinations made by Team Telecom. *March 2022 Covered List Public Notice.* That update and the most recent September 2022 updated Covered List have continued to include on that list the "covered" equipment identified in PSHSB's March 12, 2021 Public Notice on the Covered List. *See id.*; *September 2022 Covered List Public Notice.*

[653] CTA Comments at 23-25.

[654] *Id.*at 23.

[655] Dahua USA Reply Comments at 25.

assessment bodies may do so. Therefore, we find that the changes we make here are consistent with our existing MRAs.

259. More generally, we find that the possibility of retaliatory trade action is speculative, and that the expected benefits of adopting our new rules outweigh any such concerns. As mentioned above, nearly all products from China that were previously eligible for equipment authorization will remain so under our new rules, and so the impact on international trade of adopting these new rules is likely to be small.

4. Claims that Commission action is arbitrary and capricious

260. We reject the arguments of Hikvision USA and Dahua USA that the Commission's actions in this proceeding are arbitrary and capricious.[656] Hikvision USA argues that the Commission's regulations prohibition authorization of "covered" equipment is arbitrary and capricious because the regulations address highly speculative, unsubstantiated security risks about Hikvision equipment such as its video surveillance equipment, which Hikvision USA contends is secure as deployed.[657] Hikvision USA also contends that the regulations are arbitrary and capricious because of the highly disruptive effects on American businesses.[658] Among other things, Dahua USA contends that the proposed rules fall outside of the Commission's statutory authority and that the Commission should not, in any event, prohibit all of Dahua's equipment from authorization given that section 889(f)(3)(B) of the 2019 NDAA only concerns Dahua equipment to the extent used for specific purposes.[659] Considering our discussion of the record before us, and our reasoned analyses explaining the elements of the decisions that we are adopting herein with regard to Hikvision and Dahua equipment, we need not further address the claims that Hikvision USA and Dahua USA raise in general terms here.

E. Outreach

261. In the *NPRM*, the Commission sought comment on what types of actions or activities (*e.g.*, outreach and education) the Commission should take to inform all parties potentially affected by the Commission's changes to the equipment certification and SDoC rules, as well as any other rule revisions, to help ensure that they understand the changes and will comply with the prohibitions that the Commission adopts with respect to the authorization of "covered" equipment.[660]

262. As discussed above, we will provide clear guidance on the Commission's website regarding what constitutes "covered" equipment for purposes of our equipment authorization program and the prohibition on authorization that we are adopting in this Report and Order. We also noted that OET and PSHSB will issue a Public Notice on such guidance, and that any updates will also be issued pursuant to a Public Notice.

263. With regard to the revisions affecting the SDoC process in particular, we endeavor to assist each responsible party in identifying equipment that can no longer be authorized through the SDoC procedures, while also ensuring that each responsible party is accountable for any misrepresentations or violation of the prohibition that we are implementing. Because SDoC procedure does not routinely involve direct interaction with the Commission, and because the rules specify who may act as a "responsible party," in the *NPRM* the Commission asked several questions related to disseminating the

---

[656] *See, e.g.*, Hikvision USA Comments at 55-61; Dahua USA Comments at 14-17.

[657] Hikvision USA Comments at 55-61 (contending that Hikvision addresses vulnerabilities in its equipment, that fears of Chinese interventions are unfounded, and that U.S. government officials and industry professionals agree that the equipment poses no national security threat); Hikvision USA Reply at 36-44.

[658] Hikvision USA Comments at 61-65; Hikvision USA Reply at 44-54; *see also* Hikvision USA Nov. 17 *Ex Parte* at 16-20.

[659] Dahua USA Comments at 14-17.

[660] *NPRM*, 36 FCC Rcd at 10603, 10605, 10610, 10613, paras. 56, 61, 77, 88.

new SDoC limitations and requirements to the responsible parties.[661] Commenters were largely silent on those questions and, as previously discussed, the Commission does not routinely maintain information for SDoC equipment thus making direct outreach difficult. We find that because most or all entities engaged in the SDoC process are familiar with FCC procedures and their obligations to comply with our requirements, it is sufficient to provide initial notification via publication of this item on the FCC Website along with publication in the Federal Register of a summary of this change in procedure. Following implementation of the newly adopted procedures, we encourage industry and other interested parties to reach out to the Commission with any questions or concerns regarding these procedures. We direct OET to monitor such inquiries and to issue additional guidance as needed.

IV. INTERIM FREEZE ORDER

264. Because of the revisions we are adopting in the Report and Order to our part 2 equipment authorization rules and procedures to prohibit authorization of any "covered" equipment specified in the Covered List, we are also adopting an interim freeze on further processing or grant of equipment authorization applications for equipment that is produced by any entity identified on the Covered List as producing "covered" equipment. This freeze is effective on release of this Report and Order, and will last only until the Commission provides notice that the rules adopted in the order have become effective. We conclude that this action is necessary and in the public interest in order to avoid submission of new applications seeking authorization of equipment following the adoption of this Report and Order but before the rules would otherwise go into effect.[662] We take this action because "covered" equipment has been determined to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons, and the freeze accordingly serves the public interest.

265. Effective as of the adoption of this Report and Order, and because our rules, which are designed to determine which if any applications from the entities whose equipment is currently on the Covered List do not involve "covered" equipment, are not yet in effect, TCBs are directed to cease issuing equipment certifications to any of the entities identified on the Covered List – i.,e., the five named entities – Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company – and their subsidiaries or affiliates.[663] OET is directed to issue pre-approval guidance relating to the prohibition against certification of this equipment to the TCBs.[664] We remind TCBs that they were designated by the Commission "to certify equipment in accordance with Commission rules and policies," and are required to "conform their testing and certification processes and procedures to comply with any changes the Commission makes in its rules and requirements."[665] We expect that TCBs, applicants, and responsible parties will be vigilant in taking appropriate actions to implement this freeze.

266. The purpose of this interim freeze is to preserve the current landscape of authorized equipment pending the effective date of the Commission's revisions to the equipment authorization process, which will serve to protect the public interest, including the national security and public safety of United States persons. This interim procedure is consistent with our practice of taking steps to ensure that

---

[661] *NPRM*, 36 FCC Rcd at 10605, para. 61.

[662] Our decision to impose a freeze and other interim procedures is procedural and therefore not subject to the notice and comment or effective date requirements of the Administrative Procedure Act. *See* 5 U.S.C. 553b(A)-(B), (d). *See also Bachow Communications v. FCC*, 237 F.3d 683 (D.C. Cir. 2001) (affirming imposition of a freeze and interim procedures without notice and comment for applications in the 39 GHz band during transition of licensing regime); *Neighborhood TV Co., Inc. v. FCC*, 742 F.2d 629, 638 (D.C. Cir. 1984) (deeming interim processing rules, including a freeze on applications, as procedural); *Kessler v. FCC*, 326 F.2d 673 (D.C. Cir. 1963)(same).

[663] *September 2022 Covered List Public Notice*, Appendix.

[664] 47 CFR § 2.964.

[665] Amendment *of Parts 2, 35 and 68 of the Commission's Rules to Further Streamline the Equipment Authorization Process for Radio Frequency Equipment*, Report and Order, 13 FCC Rcd 24687, para. 32 (1998); *see generally* 47 CFR §S 2.960, 2.962

parties do not take advantage of the period between the adoption of new rules and the date those rules become effective.[666] The freeze will be limited to the brief time period during which the rules implementing the statutory mandate are not yet effective. Finally, if the Covered List is updated to revise the entities identified on the Covered List as producing "covered" equipment, this procedural freeze will be revised accordingly. We delegate authority to OET to modify or extend the freeze as appropriate.

V. FURTHER NOTICE OF PROPOSED RULEMAKING

A. Further Notice on Equipment Authorization

267. In this Further Notice of Proposed Rulemaking concerning the equipment authorization program (ET Docket No. 21-232), we seek further comment on some of the issues the Commission raised in the *NPRM* regarding revisions to the equipment authorization program. We also invite comment on some additional issues that have been raised with the establishment of the Commission's revised rules and approach in the Report and Order portion of this proceeding. We encourage commenters and other interested parties to submit further comments on these or other issues related to revisions to the equipment authorization to address the prohibition on authorization of equipment on the Covered List.

1. Component parts

268. In the Report and Order portion of this proceeding, we revise the Commission's part 2 equipment authorization rules to prohibit authorization of equipment that has been determined to pose an unacceptable risk to national security. Specifically, we adopt requirements for applicants for equipment certification and responsible parties authorizing equipment via the SDoC process to make attestations that the equipment for which authorization is sought is not "covered" equipment. We are not, however, requiring at this time that these attestations address the individual component part(s) contained within the subject equipment.[667] As discussed in the Report and Order, several commenters raised various concerns regarding potential practical complications and difficulties that could result from inclusion of component parts within the scope of the prohibition.[668] In this Further Notice, we seek to address these concerns as we further consider issues concerning component parts with regard to prohibitions on authorization of "covered" equipment.

269. In seeking comment on component parts, we note at the outset that we believe that certain component parts produced by entities identified on the Covered List that, if included in finished products, could potentially pose an unacceptable national security risk, similar to the security risk posed by the "covered" equipment that we are now prohibiting from authorization. Similarly, Congress, in establishing the Reimbursement Program under the Secure Networks Act shared the same concerns. It required that Huawei and ZTE equipment be destroyed as part of the rip and replace process,[669] indicating that even components of untrusted and insecure equipment could pose a danger to the United States. In the Reimbursement Program, consistent with Congressional guidance, the Commission required that

---

[666] *See, e.g., Implementation of Sections of the Cable Television Consumer Protection and Competition Act of 1992*, 8 FCC Rcd 2921 (1993) (freezing rates for cable services pending effective date of rules to avoid, among other things, cable operators raising rates "effectively undermining the statutory purpose of reasonable rates pending implementation of our rules"); *see also Revisions to Rules Authorizing the Operation of Low Power Auxiliary Stations in the 698-806 MHz Band*, Notice of Proposed Rulemaking and Order, 23 FCC Rcd 13106 (2008) (freezing the grant of equipment authorizations for low power auxiliary station devices that would operate in certain frequencies in light of the Commission's tentative conclusion not to allow low power auxiliary stations in that band); *see also AT&T, Inc. v. FCC*, 886 F.3d 1236, 1246 (D.C. Cir. 2018) ("We owe particular deference to interim regulatory programs involving some exigency.").

[667] Section III.B.2.a.

[668] *Id.*

[669] Secure Networks Act § 4(d)(7); 47 CFR § 1.50004(j). The disposal and verification requirements apply to covered communications equipment and service produced or provided by Huawei and ZTE. *See* 47 CFR § 1.50004(a)(1)-(2), (j).

categories of equipment that include components that process data be destroyed so they do not get reused and continue to pose a risk.[670] Given the challenge to protect against component parts that pose the same risk as covered equipment, we endeavor to ensure that equipment with that include component parts that pose an unacceptable risk to national security also be prohibited from authorization. In this Further Notice we seek comment to help identify such component parts and to consider how the Commission might best ensure prohibiting authorization of equipment that includes such components. In particular, we seek comment on whether and how individual component parts may need to be factored into decisions regarding authorizing equipment raises several issues that need to be more carefully evaluated to determine whether equipment with certain component parts should be considered "covered" equipment and thus prohibited from authorization. We also recognize that one complication is that many part 2 equipment authorization rules and part 15 rules reference "components," but they do so in a variety of different contexts, and there is no single or consistent meaning of the term in our rules.

270. *Background.* In the *NPRM*, the Commission proposed that component parts that comprise an RF device be considered when determining whether a device should be considered "covered" equipment and thus prohibited from obtaining an authorization. Specifically, the Commission proposed that applicants for equipment certification attest in their application (under section 2.911) that the subject equipment, including individual component parts, is not "covered" equipment.[671] The Commission also asked whether certification applications should include additional information (e.g., under section 2.1033) that would help establish that the equipment is not "covered" as a means of assisting the TCBs and the Commission with regard to approving the application, such as a "parts list" identifying the manufacturer of each component part.[672] The Commission also similarly proposed that component parts be considered when determining whether equipment is "covered" for purposes of compliance under the SDoC process.[673]

271. Several commenters express concerns about the proposal in the *NPRM* related to component parts.[674] For instance, NCTA contends that the Commission's authority under the Secure Networks Act is limited and does not support taking more granular and intrusive action such as applying any authorization prohibition to other than finished equipment products, such as component parts or software.[675] It also suggests that the Commission take a risk management approach, such as that employed by the national security agencies in addressing supply chain risks.[676] NCTA maintains that both the Secure Networks Act and section 889 of the 2019 NDAA appear to be concerned only with finished equipment products. NCTA observes that the word "component" is not mentioned in the former, and the latter uses that term to concern equipment that is a "substantial or essential component" of a network or system.[677] Moreover, NCTA argues that, in multiple portions of the Communications Act, Congress

---

[670] *Wireline Competition Bureau Announces Best Practices for Equipment Disposal and Revised FCC Form 5640 Certifications for the Secure and Trusted Communications Networks Reimbursement Program*, WC Docket No. 18-89, Public Notice, 36 FCC Rcd 14061, 14066 (WC, rel. Sept. 30, 2021) (recommending destruction and disposal of equipment that processes data as well as equipment that processes and retains data).

[671] *NPRM*, 36 FCC Rcd at 10600, para. 47.

[672] *Id.* at 10600, para. 48.

[673] *Id.* at 10605, para. 60-61. The Commission also sought comment on how to communicate to responsible parties the requirement that any equipment, including component parts, produced or provided by entities (and their subsidiaries and affiliates) that produce "covered" equipment is subject to the equipment certification process. *Id.*

[674] *See, e.g.,* CTA Comments at 16; CTIA Comments 16, NCTA Comments at 12-13; NTCA Comments at 4.

[675] NCTA Comments at 4 and 12.

[676] *Id.* at 4.

[677] *Id.* at 13 & n. 42.

expressly delineates the imposition of an obligation on equipment as well as a component thereof or software integral thereto, thereby suggesting the absence of an intention to conflate those terms.[678]

272. NTCA states that presently network providers, especially small ones, have limited ability to identify the manufacturer of every component contained within any given piece of equipment, making it difficult if they would be required to certify to the Commission that they do not have any covered equipment in their network. NTCA notes that failure to meet this obligation would also come with significant penalties, and recommends, at a minimum, that the Commission permit network providers to rely upon any determinations made by equipment manufacturers regarding what constitutes covered equipment.[679]

273. Additionally, I-PRO requests that the Commission clarify that digital device subassemblies, including computer chips, that are produced and provided by companies whose equipment is included in the Covered List do not constitute "equipment" as defined by Commission regulations and thus should continue to be exempt from equipment authorization requirements. I-Pro argues that both the proposed rule in the *NPRM* and the Commission's regulations recognize the distinction between components (such as integrated circuit chips) and the products or equipment into which such components are integrated.[680]

274. CTA expresses concern that equipment produced by any manufacturer whose products contain even innocuous components manufactured by Covered List entities would be required to go through the more burdensome certification process regardless of whether the components in those particular configurations could pose any national security risk.[681] CTA argues that a registration system or attestations could impose burdens on compliant companies manufacturing simple devices such as light switches or power tools that may have a component sourced from a Covered List entity.[682] CTA also contends that the change from SDoC to certification in those cases would cost time and resources, and potentially deter innovation with uncertain benefits, because a component being originally sourced from a Covered List entity does not mean it is a threat to security. CTA recommends that, if the Commission wants to have a more stringent process to review devices manufactured by entities that include components produced by entities on the Covered List, the Commission should revise its proposal to target those components that would impose a national security risk and avoid unnecessarily restricting the beneficial SDoC process.[683]

275. CTIA opines that it is unclear how a parts list requirement would further the Commission's national security goals because, they argue, numerous component parts have no implications for radiofrequency interference or for national security. CTIA further maintains that proposed attestation requirements also raise significant questions that were not addressed in the *NPRM*, including uncertainties about how the Commission will define and regulate component parts, and that in order to make accurate representations applicants will need more clarity about what the Commission considers to be component parts.[684]

276. Huawei contends that the Commission's continuing focus on the corporate origin and identity of equipment, rather than its security and technical specifications, overlooks the complexity of the global supply chain, where all vendors regardless of origin likely will include at least some Chinese-manufactured or produced components in their equipment. In Huawei's view, even assuming that some

[678] *Id.* at 13-14.

[679] *Id.* at 4.

[680] i-PRO Comments at 2.

[681] CTA Comments at 12.

[682] *Id.* at 21.

[683] *Id.* at 19.

[684] CTIA Comments at 16.

potentially risky equipment would be removed from the U.S. marketplace, other equipment with components originating in China or other suspect countries will remain widely available, and the overall risk to the U.S. public would be only minimally reduced.[685]

277. *Discussion.* We seek comment about the extent to which component parts should be considered as the Commission implements its prohibition on "covered" equipment in its equipment authorization program. As we consider how component parts should be treated in this process, we note that establishing a prohibition that includes considering component parts could require changes to our existing application process, which does not currently capture detailed information about the source of components that make up such equipment.[686] As this proceeding examines the equipment authorization process which is the gateway for equipment entering the U.S. marketplace with potential to ultimately become part of a telecommunication system or network, we believe it is within the purview of the statute and our duty to address all equipment on the Covered List, including component parts of devices where the inclusion of such component parts would render the equipment "covered." We seek comment on this view.

278. In seeking comment on how the Commission should address component parts with respect to the prohibition on authorization of "covered" equipment, we also invite comment on how best to address the concerns previously raised by commenters regarding component parts. As discussed above, these concerns include what the Commission would consider to be component parts for purposes of implementing any potential prohibition on equipment authorizations that include such parts, including the extent to which only some types of component parts, or all such parts, should be considered. We also seek comment on practical considerations that would be involved with extending the prohibition to include component parts, including the requirements placed on applicants for equipment authorizations to identify any particular components.

279. As discussed above, in implementing the Secure Networks Act with regard to the Reimbursement Program, the Commission determined that categories of equipment that include components that process and retain data, or that process data, be destroyed so they do not get reused and continue to pose a risk.[687] As we consider how to address components in this proceeding, we seek comment on whether we should attempt to identify ranges of components based on their risk assessment. For example, similar to the Reimbursement Program, does equipment that includes components that process and retain data, or that even process data, produced by entities identified on the Covered List, pose too much of a risk to the United States and its people to be authorized?

280. In proposing to include component parts within the scope of "covered" equipment in the *NPRM*, the Commission did not define the term and referred to both "components" and "component parts."[688] To ensure that equipment manufacturers, importers, assemblers, TCBs, and other parties associated with the Commission's equipment authorization program are clear as to what equipment may be impacted by a prohibition on component parts from entities on the Covered List, we would need to first develop and provide guidance on what component parts would need to be considered.

281. At a high level, we note that the Commission permits modules as well as composite systems (or devices) to obtain equipment certification.[689] A module generally consists of a completely self-contained transmitter that is missing only an input signal and power source to make it functional.

---

[685] Huawei Cos. Comments at 15.

[686] *See NPRM*, 36 FCC Rcd at 10600, 10604, 10605, 10612, paras 47-48, 58, 60-61, 83-84.

[687] *Wireline Competition Bureau Announces Best Practices for Equipment Disposal and Revised FCC Form 5640 Certifications for the Secure and Trusted Communications Networks Reimbursement Program*, WC Docket No. 18-89, Public Notice, 36 FCC Rcd at 14066 (recommending destruction and disposal of equipment that processes data as well as equipment that processes and retains data).

[688] *See, e.g., NPRM*, 36 FCC Rcd at 10600, paras 47-48 and 10604, para 58.

[689] 47 CFR §§ 15.212 (modules) and 2.1033(e) (composite devices).

Modules are designed to be incorporated into another device such as a personal computer.[690] The advantage of using modules is that a transmitter with a modular grant can be installed indifferent end-user products (or hosts) by the grantee or other equipment manufacturer without the need for additional testing or a new equipment authorization for the transmitter.[691] A composite system incorporates different devices contained within a single enclosure or in separate enclosures connected by wire or cable.[692] A single equipment authorization application may be filed for a composite system that incorporates devices (including modules) subject to certification under multiple rule parts.[693]Commission rules are flexible regarding the types of equipment that can be certified as modules and then incorporated into another device with no further action from the Commission and composite systems that could contain components (in this case a device). Telecommunications equipment or video surveillance equipment could contain one or more modules or could be assembled as a composite system and contain equipment produced by any of the entities (or their respective subsidiaries or affiliates) specified on the Covered List.

282. To ensure compliance with the prohibition on authorization of equipment identified on the Covered List, we seek comment on whether we should require that applicants or responsible parties, as applicable, obtain a separate equipment certification for any device that contains a module produced by any of the entities (or their respective subsidiaries or affiliates) specified on the Covered List. If the Commission were to adopt such a requirement, we seek comment as to how it should be applied. Should the Commission require that devices that incorporate previously certified modules produced by any of the entities (or their subsidiaries or affiliates) on the Covered List would need to obtain a separate equipment authorization and certify that the device is not "covered" equipment? We seek comment on this view. Would such actions be sufficient to ensure against the availability of equipment containing modules that could present a security risk? Would a policy of requiring certain devices containing modules to go through the certification process and the associated attestation requirement we are adopting in the Report and Order, strike the right balance between providing the same flexibility for delivering products to the American public as is available today for most devices containing modules while adding additional oversight on devices that could potentially be a security risk? What additional costs in terms of time or money would such a policy impose on device developers? What other approaches could be used to ensure devices containing modules do not cause a security risk to the United States and its citizens?

283. Similarly, because a composite system could be assembled by a third party and incorporate multiple devices including devices produced by any of the entities (or their respective subsidiaries or affiliates) specified on the Covered List, we seek comment on how to treat composite systems. First, recognizing that a composite system could contain only already-certified modules, we seek comment on treating them in the same manner described above for modules. That is, if any module in such a device is produced by any of the entities (or their respective subsidiaries or affiliates) specified on the Covered List, that device would be required to obtain a separate certification (including the attestation we are requiring in the Report and Order stating that the composite system does not contain any "covered" equipment). We seek comment on this approach. Second, in cases where a composite

---

[690] *See* Part 15 Unlicensed Transmitter Modules Small Business Compliance Guide, DA 08-314, ET Dkt No. 03-201, 23 FCC Rcd 2574 (2008).

[691] *See* KDB 996369 D01 Module Certification Guide v02 (available at: https://apps.fcc.gov/kdb/GetAttachment.html?id=iL3CDxZIRRPc1UBc25AGsQ%3D%3D&desc=996369%20D01%20Module%20Certification%20Guide%20v02&tracking_number=44637). In the past, modular authorizations have been limited to part 15 devices for unlicensed use. However, the Commission recently sought comment on approval guidance for split modules applicable to devices used for licensed services. *See* Draft KDB 996369 D05 Split Module DR07-44767 (available at: https://apps.fcc.gov/eas/comments/GetPublishedDocument.html?id=492&tn=370073). Comments on this draft guidance were due on Aug. 26, 2022. The Commission is evaluating comments received and anticipates future issuance of final guidance.

[692] 47 CFR § 2.947(f).

[693] *Id.* § 2.1033(e).

system contains only devices that on their own would require certification or a mix of such devices and already approved modules, we note that our rules already required such devices to obtain a separate certification. Because such devices can be assembled by parties other than the original device manufacturer, we seek comment on requiring the attestation we are adopting in the Report and Order to affirmatively state that none of the devices that comprise the composite system are on the Covered List. We do not believe such a requirement would impose any cost or undue burden on equipment certification applicants as such a requirement would be consistent with the requirements adopted in the Report and Order. We seek comment on this approach. We also seek comment on other approaches to dealing with composite systems in the certification process to ensure that such devices do not pose a security risk to the United States and its citizens.

284. We also seek comment on other broad approaches that could appropriately address concerns about component parts in our equipment authorization program. For instance, if equipment includes any component parts that could be authorized on a standalone basis, and such a component on its own would be considered "covered" equipment prohibited from authorization, then the equipment would be deemed "covered" equipment and thus prohibited from obtaining an equipment authorization. In addition, we note that if any determinations about "covered" equipment made by any enumerated source pursuant to the Secure Networks Act includes component parts, then this too would mean that equipment that includes such component parts would be "covered" equipment for purposes of our prohibition. We seek comment on this as well.

285. We believe that dealing with component parts as described above is relatively straightforward. However, focusing on component parts at a more granular level, i.e., looking at all of the individual component parts that might be used to assemble a final device, would be more complicated. As discussed above, several commenters contend that, for purposes of prohibiting authorization of "covered" equipment, many component parts would not raise security concerns.[694] We invite comment, including specific comment on whether certain types of component parts potentially raise such a concern, while others do not. For example, do passive electronic components such as resistors, diodes, inductors, etc., pose a security risk by themselves? Do random access memory (RAM) chips, whose stored data is lost once power is disconnected or turned off, or components that comprise the bus, whose function is solely to link input and output ports, pose any security risk? Should our focus instead be on those components that have the ability to examine data traffic and route such traffic or provide the instructions to do so, or might otherwise pose an unacceptable risk to national security? We include here read only memory (ROM), flash memory, the central processing unit (CPU) or any other processor within the device, and the input and output ports (as they may be able to carry out routing functions). Should we be concerned about semiconductors? Do commenters think that we should consider rules regarding other component parts and if so, what rules would be appropriate? Should the Commission here be guided by the Reimbursement Program and, rather than try to identify every type of component, simply prohibit authorization of components that process and or retain data? Notwithstanding any specific method of addressing these component parts within the equipment authorization process as described below, we seek comment on any overall approach to separating out component parts of interest that could pose a security risk versus component parts that do not. Does equipment need to be examined down to this level to ensure compliance with the prohibition on authorization of communications equipment that poses an unacceptable risk to national security under the Secure Networks Act? Should equipment that contains certain component parts produced by any of the entities listed on the Covered List be considered "covered"? If we were to adopt rules to address component parts, what types of components may need to be considered as posing an unacceptable risk to security risk? Commenters also should explain the reasons that particular component(s) would create an unacceptable risk. For example, should such components be limited to only those by being able to examine and route data or execute certain functions on an incoming or outgoing data stream? Would we need to specifically define the components of interest in our rules or would a descriptive statement suffice? For example, would it be sufficient to

[694] *See, e.g.*, CTA Comments 12; CTIA Comments at 16.

specify that any component part within a device that is capable of examining an incoming or outgoing data stream and performing routing functions falls under the umbrella of component parts of interest within the equipment?

286. In addition to categorizing the component parts that may be of interest when determining whether certain equipment should be considered covered equipment, we seek comment on how any identified component parts would be addressed in the equipment authorization process, both for certified devices and devices authorized through the SDoC process. Because parties seeking an equipment authorization must attest that the equipment in question is not "covered" equipment, how would a manufacturer, assembler, or other entity ascertain whether the components in question could result in their intended end product being covered equipment? Could an end-product produced or assembled by an entity not identified on the Covered List become "covered" equipment if it includes certain components produced by any entity identified on the Covered List? Should, as suggested by NCTA,[695] such entities producing or assembling end products themselves obtain statements from their suppliers that certain components within any products obtained for inclusion in a Commission-regulated end product for the U.S. market does not contain components that are covered equipment or that could result in a device being classified as covered equipment? If so, should such statements be required to be provided int the authorization process, and/or available to the Commission upon request? What criteria could be used to decide when such equipment should be considered "covered" equipment? Are there objective standards for determining when a final product produced by an entity not identified on the Covered List that contains at least one component part produced by an entity named on the Covered List (or any of its affiliates or subsidiaries) is considered to be "covered" equipment? To what extent must the applicant for equipment certification be responsible for knowing whether any component part of its equipment was produced by any entity identified on the Covered List? As discussed above, elsewhere within the federal government, pursuant to EO 13873, efforts are underway to address the national security risks stemming from vulnerabilities in information and communications technology (ICT) hardware, software and services.[696] Among these efforts, the Cybersecurity & Infrastructure Security Agency (CISA) established the ICT supply chain risk management (SCRM) Task Force, [697] which is working on developing a taxonomy of a "hardware bill of materials" that can be used when procuring ICT products (e.g., an inventory of elements that makes up a particular piece of equipment)[698] as well as a "software bill of materials."[699] The Task Force's efforts potentially could provide guidance and certainty in the equipment authorization process as to whether a piece of equipment complies with our rules. Should the Commission work with this Task Force to identify potential solutions to the lack of awareness of equipment components? How should this Task Force inform our own potential treatment of component parts in our equipment authorization process? Should the Commission consider an applicant's exercise of reasonable diligence in seeking to determine whether the equipment includes a component part that potentially raises national security concern be sufficient for purposes of its attestation about the whether the equipment is "covered"? What other steps could an applicant take to ensure that all component parts comply with our rules? What specific attestation should the Commission require? Would an attestation that the device is not "covered" equipment be sufficient, and should the attestation include more specific information about component parts? What additional information should an entity provide to a TCB along with the application for certification or retain with records for SDoC authorizations? How can the

[695] NCTA Comments at 4.

[696] https://www.cisa.gov/eo13873.

[697] https://www.cisa.gov/ict-scrm-task-force.

[698] https://www.cisa.gov/news/2022/01/11/ict-supply-chain-risk-management-task-force-announces-new-members-and-working-group (stating that the Hardware Bill of Materials Working Group will focus on identifying appropriate information for the development of a baseline hardware bill of materials template that organizations can use when procuring or deploying ICT products).

[699] https://www.cisa.gov/sbom.

Commission ensure that any action on components that it takes falls within the whole-of-government approach toward network and United States security?

287. We seek comment on each of these questions, and also on the overarching questions of the impact on both equipment security and the economy of considering component parts in our analysis of "covered" equipment. Specifically, we seek comment and data on the quantity and market share of entities on the Covered List in supplying modules or other devices for products intended for sale in the U.S. market, including composite devices as well as component parts as described above. We further seek comment, and encourage commenters to provide data, on the availability and costs of substitute modules, devices, and component parts from suppliers that are not identified on the Covered List, as well as the average lifespan/product cycle of affected final products. In the case that a component part may be identified as "covered" equipment, we seek comment on the feasibility and costs of replacing such component part installing a replacement component. Would taking account of component parts broadly to include modules, devices, and the building block parts that make up a device produce an overall net positive benefit, taking into account both equipment security and economic impact? Is there a particular approach to identifying component parts that would maximize net benefits, such as focusing only on those component parts or type of parts that have been determined as posing an unacceptable risk to national security or the security and safety of U.S. persons?

2. Revocation of existing equipment authorizations involving "covered" equipment

288. In the *NPRM* the Commission sought comment on the extent to which the Commission should revoke any existing equipment authorization if it adopted rules to prohibit future authorization of "covered" equipment.[700] As discussed above in the Report and Order, we conclude that the Commission has the existing authority to revoke such authorizations, including those granted prior to adoption of this Report and Order.[701] With regard to revocation of any existing authorizations of "covered" equipment, in the *NPRM* the Commission did not propose to revoke any existing authorizations (and does not do so in this Report and Order),[702] but instead sought comment on whether there are particular circumstances that would merit revocation of specific equipment, and if so, the procedures that should apply (including possible revisions to those procedures).[703]

289. In the *NPRM*, the Commission sought comment on what particular circumstances would merit Commission action to revoke any existing authorization of "covered" equipment.[704] To the extent revocation of any "covered" equipment might be appropriate, the Commission inquired about whether there was some process in which the Commission should engage to help identify particular equipment that should be considered for revocation. It recognized that in many situations the revocation of any particular equipment might benefit from an appropriate and reasonable transition period for removing the equipment, but also sought comment on whether any situations might merit immediate compliance with a revocation.[705] Further, the Commission sought comment on appropriate enforcement policies that should be associated with any revocation, including whether any monetary penalties should be considered. It also inquired whether any educational or outreach efforts should be undertaken in the event of any equipment revocation.[706] In addition, the Commission also asked about the specific procedures that the Commission should use if it seeks to revoke any existing authorization of "covered" equipment. In

[700] *NPRM*, 36 FCC Rcd at 10611, para. 82.

[701] *See* Section III.B.6, above.

[702] *See id.*

[703] *NPRM*, 36 FCC Rcd at 10611-13, paras. 83-89.

[704] *Id.* at 10612, para. 85.

[705] *Id.* at 10613, para. 88.

[706] *Id.*

particular, it noted that the existing procedures for revocation of equipment authorizations, as set forth in section 2.939(b), are the same procedures as for revocation of radio station licenses, which include several involved steps and procedures (e.g., Commission order to show cause, and opportunity for a hearing). The Commission sought comment on whether these extensive procedures would be appropriate considering that "covered" equipment has been determined to pose an unacceptable risk to national security.[707]

290. As we note in the Report and Order, many commenters raise a range of concerns about whether the Commission should revoke any existing authorizations of "covered" equipment, and we seek further comment here on the issues the Commission raised in the *NPRM* on this topic. Our further consideration here also complies with the Secure Equipment Act, in which, as discussed above, Congress recognized the Commission's authority to examine the necessity for review and possible revocation of previously existing equipment authorizations and/or to consider the Commission's rules providing for possible revocation of previously granted equipment authorizations.[708] We use this Further Notice to further explore the issues concerning equipment authorization revocation with respect to "covered' equipment authorized prior to our adoption of a prohibition on authorization of such equipment, and to expand the record on this topic, particularly in light of the actions taken and guidance provided in the Report and Order.

291. *Scope of revocation.* As noted, in the *NPRM* the Commission sought comment on whether, following adoption of the rules in the Report and Order, it should consider revoking any existing authorizations involving "covered" equipment. 5G Americas argues that a blanket rescission of existing authorizations, however worthy the security goal, would undermine trust in the Commission's processes. According to 5G Americas, there could be an inhibitive long-term effect as developers of innovative equipment choose to introduce their devices, base stations, switches, and components in markets outside the United States.[709] Many commenters also generally oppose action by the Commission to revoke existing authorizations of "covered" equipment, expressing various concerns such as the potential for adverse impact to consumers and the supply chain.[710] IPVM, on the other hand, advocates that the Commission revoke authorizations if the equipment would now be considered "covered" equipment.[711] We seek comment on the scope of possible revocation of existing authorizations that it should consider, and whether there might be situations that would warrant revocation in certain circumstances.

292. *Identification of devices that possibly should be revoked*. In considering whether any existing equipment authorizations of "covered" equipment should be revoked, the Commission sought comment on whether there should be some process in which the Commission should engage to identify particular equipment authorizations that should be considered for revocation. It invited commenters to suggest such a process. It also asked whether the Commission should rely on outside parties' reports in its considerations. The Commission recognized the need to avoid taking any actions that would be

[707] *Id.* at 10612-13, para. 87.

[708] Secure Equipment Act § 2(a)(3)(B)(1)-(2).

[709] 5G Americas Comments at 3.

[710] *See, e.g.*, CTA Comments at 14 (could be disastrous for consumers); CTIA Comments at 9-12 (could present serious challenges potentially harming American consumers, and could weaken supply chains); ITI Council Comments at 5-8 (revocation of "covered" equipment would unmoor the revocation process, present a myriad of practical challenges as well as industry and consumer confusion); NCTA Comments at 9-10 (would create an unfunded "rip" and "replace" mandate); NTCA Comments at 7 (would be highly detrimental to providers that relied on the Commission's rules); TIA Comments at 12 (only proceed if a mechanism exists to reimburse those affected). We note that the People's Republic of China argues that the equipment authorizations that have been previously granted strictly followed the then-effective regulations, and thus there could be no violation of section 2.939. PRC Comments at 3.

[711] IPVM Jan. 11, 2022 *Ex Parte* at 4-5.

overbroad in terms of affecting users of the previously-authorized equipment or would require removal of this equipment faster than it reasonably can be replaced.[712]

293. TIA states, for instance, that a cost-benefit analysis is necessary to ensure that revocation would be in the public interest.[713] CTIA expresses concern that revoking existing equipment authorizations threatens to inject complexity into the Commission's "remove and replace" proceeding.[714] Clete Johnson and Jennifer Tatel argue that revocation of previous authorizations would create significant problems that would outweigh the potentially marginal security benefits of mandating and accelerating the unfunded removal of existing covered equipment.[715] We also note that Huawei, Dahua, and Hikvision representatives each argue that revocation of any existing authorizations could raise constitutional claims.[716]

294. Some commenters suggest that revocation of existing authorizations might involve some sort of reimbursement for affected industry and consumers. TIA recommends that, should some revocation be required for national security purposes, the Commission should work with its partners in industry and press Congress to authorize and appropriate funds to make affected parties whole, should the extreme step of revocation be the best option to serve national security,[717] while US Telecom contends that a new program for reimbursement would need to be established by Congress to enable revocation.[718] CTIA also expresses the need for addressing funding issues (noting that any formal replacement process would likely require a legislative solution),[719] and the need for the Commission to be predictable.[720] Clete Johnson and Jennifer Tatel argue that, absent a funded program for replacement and reimbursement, the potential for revocation could raise extremely complex and disruptive challenges, including recalls and unfunded mandates to identify and replace equipment that in the future might be subject to revocation.[721]

295. In light of these issues, we seek further comment on whether there should be some process for identifying particular "covered" equipment whose authorization should be revoked because its continued authorization poses an unacceptable risk to national security.[722] We note that the Commission previously has authorized equipment produced by the companies producing equipment on the current Covered List, and we anticipate that additional equipment produced by other companies may be determined to pose an unacceptable risk to national security and added to the Covered List as that list is updated in the future. How might the Commission or others identify existing authorizations among these if considering whether some of this equipment might merit revocation? Are there any specific cases of equipment that might merit immediate revocation? To what extent should the risk of such equipment to national security be considered, and how could such risk be evaluated? What are the benefits of eliminating this risk and the associated costs of revoking equipment necessary to eliminate this risk? As

---

[712] *NPRM*, 36 FCC Rcd at 10613, para. 88.

[713] TIA Comments at 11-13.

[714] CTIA Comments at 11-12.

[715] Johnson and Tatel Comments at 4.

[716] *See, e.g.*, Dahua USA Comments at 18-21 (raising retroactivity and due process concerns); Huawei Cos. Comments at 34-35, 37-38 (raising retroactivity and due process concerns); Hikvision USA Reply at 56-57 (raising takings concerns).

[717] TIA Comments at 11-13.

[718] US Telecom Comments at 5.

[719] CTIA Comments at 10.

[720] *Id.* at 12.

[721] Johnson and Tatel Comments at 4.

[722] We seek comment on the constitutional claims raised by Huawei, Dahua, and Hikvision below, when discussing the applicable process for revoking any existing equipment authorization.

stated earlier, we conclude that the Commission has the authority, as affirmed by Congress in the Secure Equipment Act, to consider the necessity to review or revoke an existing authorization of "covered" equipment approved prior to adoption of this Report and Order, and that it has such authority to consider such action without considering additional rules providing for any such review or revocation of existing authorizations. Considering the potential risk to national security concern, should the Commission consider revoking all authorizations of "covered" equipment, and if so how would such a potential revocation would be implemented given the wide variety of existing authorizations? Also, to what extent should revocation of any particular equipment depend on establishment of a reimbursement program?

296. *Considerations related to revocation of existing authorizations.* In the event the Commission concluded that revocation of an equipment authorization may be appropriate, the Commission sought comment on the appropriate and reasonable transition period that may be necessary.[723] We note that such revocation might take different shapes. For instance, the revocation potentially could go so far as to involve not only prohibiting the future manufacture, importation, marketing, and sale of specified devices, but also requiring that the equipment no longer be used. On the other hand, the revocation could conceivably be partial and limited, such as a revocation of an existing authorization that could, at some time in the future, preclude further import, marketing, or sale of the affected equipment.

297. If we decide that revocation of existing authorizations is necessary, we request additional comment on determining an appropriate transition period and whether and how that might depend on the scope of the revocation and the particular equipment involved. CTIA, for instance, recommends that the Commission ensure that there is an adequate "runway" for decommissioning devices that are already in the market at the time of revocation and ensure that carriers can adequately support devices until they are phased out (e.g., through security patching) to mitigate the risk of these devices becoming less secure or targets for bad actors.[724] ITI states that, if the Commission were to move forward with its revocation proposal, it is critical that an adequate transition period be established that takes into account the many complex variables that relate to identifying, sourcing, and replacing the equipment, along with the Commission's own capacity to manage such a process.[725] Should the Commission provide a suitable amortization period for equipment already in the hands of users?[726] To what extent might the expected life-cycle of the equipment be taken into account? Pursuant to section 2.939(c), which provides for the revocation of any equipment authorization in the event of changes in its technical standards, we previously sought comment on the provision of a suitable amortization period for equipment already in the hands of users or in the manufacturing process, and invite further comment here.

298. We also seek comment on the extent to which issues related to the supply chain might figure in the Commission's considerations. CTIA, for instance, contends that revocation of previously approved equipment may also weaken supply chains by impacting mutual recognition agreements (MRA) that industry relies on to facilitate trade in telecommunications equipment.[727] In ITI's view, in revoking existing authorizations the Commission should consider market conditions and potential equipment delays, including increased demand for connected devices, and also address the additional supply chain

[723] *NPRM*, 36 FCC Rcd at 10613, para. 88.

[724] CTIA Comments at 13.

[725] ITI Comments at 11.

[726] Pursuant to section 2.939(c), which provides for the revocation of any equipment authorization in the event of changes in its technical standards, the Commission previously sought comment on the provision of a suitable amortization period for equipment already in the hands of users or in the manufacturing process. *NPRM*, 36 FCC Rcd at 10612-13, para. 87.

[727] CTIA states that MRAs allow participating countries to agree to accept the test results or product approvals performed by the Conformity Assessment Bodies of another country, thus reducing burdens on manufacturers and speeding time to market, and that revocations by the Commission could undermine the MRA construct or frustrate their ongoing administration. CTIA Comments at 12.

pressures that would occur should existing equipment authorizations be revoked.[728] How might the Commission evaluate supply chain issues in its consideration of whether to revoke an existing authorization, and if so what information and data (e.g., number of devices, market share, substitutes, and prices) might be useful to such a consideration?

299. How should consumer-related concerns be factored in? CTIA raises concerns relating to consumers. CTIA states that revoking existing authorizations for consumer products without a mechanism for removing them from the market would create significant confusion for consumers and could pass significant costs on to consumers who would presumably be placed in the difficult position of needing to replace newly-unauthorized devices.[729] CTIA further argues that building a mechanism to remove retroactively de-authorized devices from the market would be complex and would need to consider how consumers would be made aware of the need to replace devices.

300. As noted above, there could be more than one type of revocation of existing equipment authorizations. Many commenters express concerns in the event the Commission revoked an existing authorization and required users to stop using that equipment. The Commission also might consider a kind of partial revocation of an existing authorization, such as in the case in which, at some specified date in the future, the importation, sale, or marketing of equipment that had previously been authorized could be prohibited. Such an action could eliminate any costs on users that would be associated with a requirement that existing equipment be replaced, while also promoting national security by preventing further purchasing and use of "covered" equipment that has been determined to pose an unacceptable risk to national security. We seek comment on the market impact of various types of revocation mentioned above, including estimates of the impact on costs and availability of equipment. We also seek comment on how the transition period for any such revocation affect the costs of revocation and availability of equipment.

301. To what extent should the time at which the equipment authorization was initially granted be a factor? For instance, IPVM contends that, to the extent that some equipment that could no longer be authorized under the rules and procedures adopted in this Report and Order may only recently have been authorized (such as in the months immediately before adoption of these new rules), it would be reasonable for the Commission to revoke such authorizations; IPVM notes that in these cases revocation of the equipment would have minimal impact on American end-users because most of these products have not yet been widely sold or installed.[730] We seek comment, including on the extent to which "covered" equipment has been authorized recently (e.g., after issuance of the *NPRM*, or at any time before the rules adopted in this Report and Order go into effect). Alternatively, to the extent that the equipment was authorized many years ago and has surpassed its expected life-cycle, might that be more reasonable grounds for the Commission to revoke the authorization?

302. Also, we note that there might be other alternatives to that of requiring complete revocation of an authorization. For instance, might there be measures, such as requiring the particular components of equipment be replaced or certain security patches be implemented, that might avoid the need to replace equipment that had been previously authorized? If so, how would such an approach be implemented? Should estimated costs associated with these alternative measures be taken into account? If so, we seek comment and quantitative data associated with the costs of the alternative measures. Finally, we request any additional thoughts on other considerations that the Commission should take into account with regard to potential revocation of particular existing authorizations.

---

[728] ITI Comments at 11.

[729] CTIA Comments at 10.

[730] IPVM Jan. 11, 2022 *Ex Parte* at 3-5. IPVM states its understanding that Hikvision and Dahua have filed a high number of equipment authorization applications since the time that the initial Covered List that identified those entities as producing "covered equipment was first published by PSHSB in March 2021. *Id.*

303. *Procedures for revocation.* In the *NPRM*, the Commission asked whether the Commission should revise or clarify the existing processes for revocation set forth in section 2.939(b) with regard to existing authorizations of "covered" equipment, given that the equipment has been determined to pose an unacceptable risk to national security.[731] Under section 2.939(b), the procedures for revoking an equipment authorization are the same procedures as revoking a radio station license under section 312 of the Communications Act.[732] Section 2.939(b) requires that revocation of an equipment authorization must be made in the "same manner as revocation of radio station licenses,"[733] and thus generally would include the requirement that the Commission serve the grantee/responsible party with an order to show cause why revocation should not be issued and must provide that party with an opportunity for a hearing.[734] As discussed above in the Report and Order, however, applying section 312's procedures to revocation of equipment authorizations is not statutorily required.[735]

304. Hytera recommends that, if the Commission pursues revocation of existing authorizations, it should provide full and complete due process protections for the holders of the authorizations as spelled out in section 2.939(b).[736] We note that Huawei, Dahua, and Hikvision also object to any revocation of existing equipment authorizations premised on potential constitutional claims related to due process.[737] In considering the serious concerns surrounding equipment on the Covered List, the Commission seeks additional comment on the potential for expedited or otherwise different procedures for revocation of "covered" equipment. We seek comment on the necessity for section 312 procedures, which apply to the revocation of a "station license or construction permit" as defined in the Act, to apply with respect to revocation of any existing "covered" equipment. Should the process we adopt in new rule 2.939(d) apply more broadly to existing equipment authorization revocations? We also seek comment on the scope of any due process or other constitutional requirements for such revocation procedures.

305. *Enforcement.* In the *NPRM*, the Commission sought comment on enforcement issues that could arise if the Commission revoked equipment authorizations.[738] It noted that, pursuant to section 503(b)(5) of the Act,[739] the Commission must first issue citations against non-regulatees for violations of FCC rules before proposing any monetary penalties. Such citations "provide notice to parties that one or more actions violate the Act and/or the FCC's rules – and that they could face a monetary forfeiture if the conduct continues."[740] In contrast, pursuant to section 503(b)(1)(A) of the Act,[741] the Commission may assess a monetary forfeiture against grantees for violations of our rules without first issuing a citation. Therefore, the Commission may take enforcement action against a grantee who continues to market equipment after the authorization for that equipment has been revoked. We also note that third party suppliers, importers, retailers, and end users (i.e., non-regulatees), who are not Commission regulatees,

---

[731] *NPRM*, 36 FCC Rcd at 10612-13, para. 87.

[732] *See* 47 CFR § 2.939(b); 47 U.S.C. § 312.

[733] 47 CFR § 2.939(b).

[734] *See* 47 U.S.C. § 312(c).

[735] *See* Section III.B.6.a, above.

[736] Hytera Comments at 12.

[737] See, *e.g.*, Huawei Comments at 34-35, 37-38 (raising retroactivity and due process concerns); Dahua Comments at 18-19, 20-21 (raising retroactivity and due process concerns); Hikvision Reply at 56-57 (raising takings concerns).

[738] *NPRM*, 36 FCC Rcd at 10613, para. 88.

[739] 47 U.S.C. § 503(b)(5).

[740] *See* Federal Communications Commission, Enforcement Bureau, "Enforcement Overview" at 10*, available at* https://www.fcc.gov/sites/default/files/public_enforcement_overview.pdf (last visited June 14, 2021).

[741] 47 U.S.C. § 503(b)(1)(A).

may not be aware that they are subject to Commission rules. Similarly, such non-regulatees may not be aware when equipment they market or use has been revoked by the Commission.

306. We seek comment on the best enforcement mechanisms the Commission should employ to swiftly curb the potential for post-revocation equipment marketing or use by such parties. Are there obligations that could be imposed on grantees or responsible parties that would help alleviate these concerns? We also seek comment on how the Commission might revise its rules or work with federal partners and the communications industry to address existing covered equipment that may be in the marketplace post-revocation without adversely affecting consumers and others downstream in the supply chain? We seek further comment on these issues, as well as any comment that could help the Commission enforce the requirements imposed following revocation, such as an appropriate enforcement policy for the continued marketing, sale, or operation of equipment if the revocation involves a transition period.

307. *Other revisions*. We again request comment on whether the Commission should make any other revisions to section 2.939 that would address revocation of "covered" equipment. Should specific provisions be included that focus on revocation of equipment that involve the types of equipment prohibited based on an unacceptable risk to national security? Do these concerns merit particular procedures commensurate with the risk to national security? If so, we ask that commenters provide details and explain the rationale with the suggestions.

308. *Outreach.* In the *NPRM*, the Commission asked about whether it should undertake any educational and outreach efforts to inform the public regarding any revocations of "covered" equipment that may be made, such as regarding the legal effect of revocations.[742] We did not receive any comments on this particular question and again invite comment on this issue.

3. Supply chain considerations

309. In commenting on the proposals in the *NPRM*, some commenters ask whether, in the event that there are additions of "covered" equipment to the Covered List, the Commission should consider the potential impact of certain prohibitions where immediate implementation of a prohibition could result in supply chain problems. For instance, Drone Deploy expresses concerns that certain equipment used by U.S. businesses may be produced by only a few suppliers, and that in the event that equipment from such suppliers is placed on the Covered List, urges the Commission to consider providing clear market signaling and adequate notice before such a prohibition on authorization takes effect, so as not to harm US businesses.[743] Drone Deploy further asks that the Commission work with other federal agencies in promoting the development of alternatives to equipment that may ultimately be added to the Covered List and to consider the market realities and ensure that adequate alternatives exist before restrictions on authorizations take effect.[744]

310. We seek comment on whether the Commission should, in certain instances, take into account how the prohibition of particular "covered" equipment if such a prohibition could, if implemented immediately without sufficient advance notice or opportunity for the development of alternative sources of equipment, have a deleterious effect on the public interest.

---

[742] *NPRM*, 36 FCC Rcd at 10613, para. 88.

[743] Drone Deploy Apr. 6, 2022 *Ex Parte* at 1-2. Specifically, Drone Deploy note that a single supplier produced that great majority of drones (over 90%) that Drone Deploy software uses, and that if equipment from that supplier (DJI) were placed on the Covered List, the prohibition on authorization of that equipment could undermine U.S. businesses, such as Drone Deploy and other commercial interests, that currently rely on these products. *Id.*; attachment (Policy Brief Deck) at 6-8.

[744] Drone Deploy Apr. 6, 2022 *Ex Parte* at 1-2.

4. United States point of presence concerning certified equipment

311. As noted above, in seeking comment in the *NPRM* on actions that the Commission should take that would better ensure compliance with, and enforcement of, Commission rules, the Commission proposed requiring that the party responsible for compliance with the Commission's certified equipment rules have a party located within the United States that would be responsible for compliance, akin to the current requirement applicable for equipment authorized through the SDoC process.[745] The Commission observed that if there were a responsible party for certified equipment that has a physical presence in the United States, this would allow the Commission to conduct timely investigations and readily take effective enforcement action in instances of noncompliance, including noncompliance with the requirements promulgated in this proceeding.[746] Only one commenter, Hytera US, provided direct comment in response to the Commission's proposal, supporting the identification of a U.S.-based responsible party.[747]

312. We continue to believe that it is important for the Commission to facilitate enforcement of our rules and that requiring a U.S.-based responsible party for certified equipment would represent a significant step in achieving this goal. Our actions in this proceeding to prohibit future authorization of "covered" equipment that poses an unacceptable risk to national security underscore the need for effective enforcement of applicable rules associated with certified equipment. Many certified devices that are imported to and marketed in the United States are manufactured in foreign countries and grantees of equipment authorizations with those devices are located outside of the United States. It can be difficult to effectively communicate with grantees, particularly foreign-based grantees, to engage in relevant inquiries, determine compliance, or enforce our rules when appropriate. Accordingly, it is important to have a reliable and effective means by which we can readily identify and directly engage the grantee of an FCC equipment certification, which would be facilitated by requiring a U.S.-based presence for associated with certified equipment.

313. Under current equipment certification rules, set forth in section 2.909(a), the grantee obtaining the certification is the responsible party, and the only party responsible for compliance with applicable Commission requirements concerning that equipment.[748] Requiring that, for certified equipment, there be a responsible party in the United States, would require revisions to our rules. In the *NPRM,* the Commission proposed adopting a general requirement that all applicants for equipment certification have a responsible party located in the United States, which could help ensure compliance with appliable Commission rules regarding the authorized equipment.[749] At a minimum, such a requirement would require that any grantee that resides outside the United States to designate a party

---

[745] *NPRM*, 36 FCC Rcd at 10603, para. 54; *see also* 47 CFR §§ 2.909(b), 2.1077(a)(3) (both regulations require the responsible party for SDoC equipment to be located in the United States). In the earlier rulemaking promulgating these rules, the Commission proposed to require the responsible party for certified equipment to be similarly located in the United States; however, the Commission did not adopt that proposal in 2017, and it remains pending in that proceeding. *Amendment of Parts 0, 1, 2, 15, and 18 of the Commission's Rules Regarding Authorization of Radiofrequency Equipment*, ET Docket No. 15-170, First Report and Order, 32 FCC Rcd 8746, 8772, para. 58 (2017).

[746] *NPRM*, 36 FCC Rcd at 10602-03, para 54. Under existing rules, the responsible party for certified equipment holds the obligation to ensure the compliance of its equipment. *See* 47 CFR § 2.909(a) (stating that the responsible party is "responsible for the compliance of the equipment with the applicable standards"). Entities holding authorizations issued by the Commission also can be held liable for failing to comply with the terms and conditions of the authorizations. *See* 47 U.S.C. § 503(b)(5) (granting the Commission the authority to issue a forfeiture against entities that hold or are required to hold Commission authorizations).

[747] Hytera US Comments at 13.

[748] 47 CFR § 2.909(a). Under the SDoC rules, the responsible party may be one of several entities, including the manufacturer, the importer, the retailer. *Id*. § 2.909(b).

[749] *NPRM*, 36 FCC Rcd at 10602-03, para. 54.

located within the United States that would have legal responsibility concerning compliance with such rules.

314. We request comment on the appropriate approach to implementing a U.S.-based responsible party requirement, as well as the details of implementing the approach in our rules. We believe that it remains important that the grantee of the equipment authorization always be a responsible party for ensuring compliance under our rules, as this helps ensure that there are a wide range of tools available to the Commission that can be leveraged with respect to the grantee to help promote compliance. If the grantee continues to be a responsible party, but is not located in the United States and therefore names a separate entity located in the United States as a responsible party, how would this affect our goal of promoting compliance? Would this result in there being two responsible parties? Under this approach, what would be the relationship between the U.S.-based responsible party and the grantee, and should we impose certain minimal requirements on that relationship? Would the grantee and the U.S.-located responsible party act as a co-equal in responsibility for compliance? Would both the applicant (if foreign-based) and designated U.S.-based responsible party have to attest and sign the FCC Form 731 application for equipment certification or would a single attestation be sufficient?

315. Should we revise section 2.909(a) concerning the responsible party for certified equipment to more closely align with the approach concerning responsible parties set forth in section 2.909(b), i.e., the rule already in place for equipment authorized under the SDoC process. Are there important differences between certified equipment and SDoC-authorized equipment that should be taken into consideration as the Commission considers requiring a U.S. point of presence for certified equipment? Under the SDoC approach, the responsible party must be located in the United States, and could be, depending on the situation, the manufacturer, the assembler, the importer, or the retailer.[750] Specifically, we note that under 2.909(b), if the manufacturer or assembler of the equipment is not located in the United States, and the equipment is imported, the importer of the equipment would be the responsible party unless the retailer(s) in the U.S. enter into agreement(s) with the importer or manufacturer (or assembler) to become the new responsible party.[751] We seek comment on the extent to which a similar approach should be adopted for certified equipment. Should the Commission consider requiring that the importer, the retailer, the distributor, or some other entity be the U.S.-located responsible party? Should there only be one U.S.-located responsible party permitted? We seek comment on these issues and the rules and implementation details that commenters request that the Commission consider.

316. If we require a U.S.-located responsible party, how do we ensure that any designated U.S.-based responsible party has the requisite qualifications, necessary organizational or corporate authority, capabilities, abilities and connection to the grantee to enable it to appropriately and fully respond to Commission inquiries and remedy violations of the Act and the Commission's rules? Should we, for instance, require there be a formal agreement between the responsible party and the grantee? Should we specify a particular status for the U.S.-based responsible party (i.e., a citizen, a lawful resident, etc.)?[752] What minimum criteria should we consider for a U.S.-based responsible party's physical presence in the United States? Should we require some form of financial security to ensure the Commission's ability to enforce our rules? How should the Commission collect and maintain information on any designated responsible party, through the TCB or directly with the Commission? What requirements are needed to ensure the grantee and/or the U.S.-based responsible party keeps its contact information up-to-date with the Commission? We note that these possible procedures could

[750] 47 CFR § 2.909(b).

[751] *Id.* § 2.909(b)(1)-(3). We also note that, under § 2.909(b)(4), if the equipment is modified by any party not working under the authority of the responsible, the party performing the modifications becomes the responsible party. *Id.* § 2.909(b)(4).

[752] A "non-resident" refers to any person or entity that does not permanently reside within the United States, as defined in 47 U.S.C. § 153(58).

require updating FCC Form 731 and EAS procedures to address this additional entry and require necessary updating if there are any subsequent changes.

317. Noting the rule we adopt today requiring that the applicant designate a U.S.-based agent for service of process,[753] if we adopt a requirement to have both a U.S.-based responsible party and a U.S.-based agent for service of process, is there any reason for the U.S.-based responsible party and a U.S.-based entity for service of process to be the same designee or should they be different designees? In order to effectuate enforcement over time, should the grantee be required to maintain a U.S.-based responsible party for a certain period of time after the grantee ceases marketing the device?

318. Finally, as we consider which approach to take, we seek comment on the burdens placed on applicants and the TCBs in implementing the appropriate approach.

5. Other issues

319. Now that the Commission's revised rules and approach have been established in the Report and Order above, commenters and other interested parties may wish to submit further comments on these issues or other issues. We seek further comment on some of the issues the Commission raised in the *NPRM*. We also invite comment on additional issues.

320. *Additional information under section 2.1033.* In the *NPRM*, the Commission asked whether to require the applicant to provide, under section 2.1033, additional information (possibly including a parts list) that could help establish that the equipment is not "covered" in order to assist TCBs and the Commission in the effort to prohibit authorization of "covered" equipment.[754] If so, what additional information might be helpful or appropriate, and how should the requirement be crafted to mitigate any undue burden on applicants?

321. *Review of the equipment authorization post-grant.* Noting that following a TCB's grant of certification the Commission will post information on that grant "in a timely manner" on the Commission-maintained public EAS database,[755] and that the TCB or Commission may set aside a grant of certification within 30 days of the grant date if it is determined that such authorization does not comply with applicable requirements or is not in the public interest,[756] the Commission invited comment on whether it should consider adopting any new procedures for gathering and considering information on potentially relevant concerns that the initial grant is not in the public interest and should be set aside.[757] In particular, it asked about the extent to which interested parties, whether the public or government entities (e.g., other expert agencies) should be invited to help inform the Commission as to whether particular equipment inadvertently received a grant by the TCB and is in fact "covered" equipment such that the grant should be set aside.[758] We note that commenters generally oppose establishing any new procedures.[759] We will, however, invite further comment about whether procedures for a post-grant review process should be established now that the specific new rules and procedures have been adopted.

322. *Post-market surveillance.* The Commission also sought comment on whether the Commission should consider any revisions or clarifications to the section 2.962(g) rules concerning

[753] *See supra* Section III.B.2.b.

[754] *NPRM*, 36 FCC Rcd at 10600, para. 48.

[755] 47 CFR § 2.941.

[756] 47 CFR § 2.962(f)(6).

[757] *NPRM*, 36 FCC Rcd at 10601, para. 50.

[758] *Id.*

[759] *See, e.g.*, CTIA Comments at 20 (absent additional resources and staffing, low-risk and no-risk equipment may face significant delays in obtaining approval; the cost of TCB services is likely to rise); Hytera Ltd., Power Trunk, and Hytera US Nov. 11, 2021 *Ex Parte* at 2 (post-grant challenges from third parties are fraught with potential for abuse, but if allowed, there must be due process for equipment authorization applicants).

"post-market surveillance" activities with respect to products that have been certified. Those rules currently require TCBs to perform appropriate post-market surveillance activities with respect to testing of sample of certified equipment for compliance with technical regulations.[760] The Commission noted that OET has delegated authority to develop procedures that TCBs will use for performing such post-market surveillance, and sought comment whether any revisions or clarifications that should be adopted with respect to post-market surveillance.[761] CTIA expresses concern that increasing the scope of TCBs' post-market surveillance responsibilities could result in delays in authorizing equipment and higher TCB costs.[762] Again, now that the particular rules and procedures for prohibiting authorization of "covered" equipment are now being established, we invite additional comment on this issue. Beyond the existing requirements under section 2.962(g), are there particular additional activities that TCBs should conduct in light of the goals of this proceeding?

323. *Certification process for equipment that is prohibited from using SDoC.* In the Report and Order portion of this proceeding, we adopted a rule prohibiting any of the entities named on the Covered List as producing "covered" equipment, and their respective subsidiaries or affiliates, from using the SDoC process to authorize any equipment – not just "covered" equipment identified on the Covered List. Thus, any equipment eligible for equipment authorization that is produced by any entities so identified on the Covered List, or their respective subsidiaries or affiliates, must be processed pursuant to the Commission's certification process, regardless of any Commission rule that would otherwise permit use of the SDoC process.

324. While we maintain our belief that the implementation of this rule is not unnecessarily burdensome, we did note in adopting it that as the Commission, industry, and manufacturers gain more experience over time on the effectiveness of its procedures concerning "covered" equipment, the Commission may wish to revisit this process.[763] As such, we take this opportunity to seek comment on alternative procedures that the Commission could consider to maintain oversight over equipment identified on the Covered List, while ensuring consistent application of our equipment authorization procedures. What procedures should the Commission consider to specifically address the authorization of equipment produced by entities named on the Covered List as producing covered equipment? What specific aspects of the standard SDoC process and the Certification process should the Commission combine to ensure the necessary oversight for the Commission to readily identify and address equipment of concern?

325. *Enforcement.* In light of the rules and approach that we are adopting in the Report and Order, we invite comment on other actions the Commission should consider to promote enforcement of the prohibitions in our equipment authorization program relating to "covered" equipment.

326. *Other issues*. Finally, we invite comment on other rules or procedures that the Commission should consider as it moves forward with implementation of the prohibition on authorization of "covered" equipment.

B. Further Notice on Competitive Bidding

327. In addition to considering revisions to the Commission's equipment authorization program (the subject of the Report and Order above), the Commission sought comment in the *NPRM* on whether to "require an applicant to participate in competitive bidding [for Commission spectrum licenses] to certify that its bids do not and will not rely on financial support from any entity that the Commission

[760] 47 CFR § 2.962(g).

[761] *NPRM*, 36 FCC Rcd at 10601, para. 51; *see* 47 CFR § 2.962(g).

[762] CTIA Comments at 19-20.

[763] Section III.B.3.a.

has designated under section 54.9 of its rules as a national security threat to the integrity of communications networks or the communications supply chain."[764]

328. If adopted, such a requirement could prevent the entities designated pursuant to section 54.9 from influencing the bidding in an auction for Commission spectrum licenses. The Commission has designated Huawei and ZTE, and their subsidiaries, parents, or affiliates, pursuant to section 54.9. In doing so, the Commission noted Huawei's and ZTE's ties to the Chinese government and military apparatus, along with Chinese laws obligating those companies to cooperate with any Chinese government requests to use or access their systems.[765] It also is well-established that the Chinese government helped fuel Huawei's growth by deploying powerful industrial policies to make Huawei equipment cheaper to deploy than the alternatives.[766] These policies include both direct subsidies to Huawei and state-funded export financing.[767] The Chinese government support for Huawei has been repeatedly documented.[768]

329. Indirect subsidies may include "[d]istortionary financing intended to support participation in spectrum auctions of network operators who then deploy covered equipment and services [and thereby] may raise concerns about risks to the national security of the United States and the security and safety of United States persons."[769] In the *NPRM*, the Commission noted concerns that such financing had enabled a party to outbid others for spectrum licenses at auction, effectively blocking other equipment providers.[770] It sought comment on whether a potential certification might address the risk of such distortionary financing in Commission auctions.

330. Only a handful of commenters responding to the *NPRM* address the potential auction certification. None dispute the potential risk, though each raises different concerns with a certification requirement and each offers different suggestions to address those concerns. Addressing the potential difficulty of identifying the ultimate sources of financing, Jordan Brunner suggests that the Commission accept a certification based on reasonable belief "after sufficient due diligence."[771] CTIA alternatively proposes that the certification only apply to applicants receiving "financial support" of greater than 10%, though it does not detail how this is to be measured.[772] CTIA also notes some risk that the potential certification may interfere with allowing market forces to determine the use of spectrum by artificially limiting the number of applicants seeking the licenses.[773] Echoing CTIA's concern with the breadth of the potential certification, US Telecom suggests that the certification concern only those funds "specifically

---

[764] *NPRM*, 36 FCC Rcd at 10614-15, para. 96. Under section 54.9 of our rules, the Commission may designate "a company [as] pos[ing] a national security threat to the integrity of communications networks or the communications supply chain," and thereby prohibit the use of Universal Service Fund support to purchase equipment produced or provided by that company. 47 CFR § 54.9. The rules for such designations, focused on companies, were adopted prior to the establishment of the Covered List, focused on equipment and services.

[765] *See Huawei Designation Order*, 35 FCC Rcd at 6609-16, paras. 13-27; *ZTE Designation Order*, 35 FCC Rcd at 6637-42, paras. 10-18.

[766] Chuin-Wei Yap, *State Support Helped Fuel Huawei's Global Rise*, Wall Street Journal (Dec. 25, 2019), https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

[767] *NPRM*, 36 FCC Rcd at 10614, para. 92.

[768] *See id.* at 10614, para. 93, n.240, Jill C. Gallagher, *U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy, and Economic Interests, R47012*, Congressional Research Service, Jan. 5, 2022, at 8-10.

[769] *NPRM*, 36 FCC Rcd at 10614, para. 95.

[770] *Id.* at 10614, paras. 93-94.

[771] Brunner Comments at 29.

[772] CTIA Comments at 15.

[773] *Id.*

for the purpose of auction participation."[774] US Telecom further recommends limiting the certification to those entities specifically designated, and proposes clarifications that subsequent changes in the list of those designated would have no effect on earlier certifications. Mr. Brunner, on the other hand, proposes expanding the entities covered by the certification to include relevant Chinese financial institutions.[775] Finally, rather than focus on financing, JVCKenwood USA Corp. would refocus the certification and make it into a bar on specific entities participating in Commission spectrum license auctions or the use by auction winners of equipment provided by those entities.[776]

331. Concerns about Huawei and ZTE and the risks posed by their equipment have continued since adoption of the *NPRM* and submission of the record in response, both in connection with spectrum license auctions and more generally. Concerns about the security of Huawei equipment were a significant topic in connection with Brazil's 2021 auction of spectrum licenses for use with 5G wireless technology.[777] More recently, separate from any license auction, Canada issued a ban on equipment from Huawei and ZTE with respect to all licenses.[778]

332. In light of the record in response to the *NPRM*, continuing concerns regarding Huawei and ZTE, and today's action with respect to equipment certification, we seek further comment on the risk of distortionary auction financing and potentially addressing that risk with a required auction application certification. Given developments since the *NPRM*, including the steps taken with respect to equipment approvals, has the risk of distortionary auction financing to benefit section 54.9 companies lessened or increased? As additional actions are taken with respect to untrusted equipment and vendors, is a potential auction certification more or less likely to be effective in addressing the underlying concern? As noted in response to the *NPRM*, such an inquiry can be difficult to tailor to address the underlying concern without imposing a burden on or creating uncertainty for auction participants. Would any of the alternatives suggested in the record address the underlying risk more effectively? Are there alternative ways to narrow or otherwise target the certification that would address the national security concerns, while limiting any negative impacts on competitive bidding?

VI. PROCEDURAL MATTERS

333. *Final Regulatory Flexibility Analysis*. As required by the Regulatory Flexibility Act of 1980 (RFA),[779] as amended, the Commission has prepared a Final Regulatory Flexibility Analysis (FRFA) regarding the possible significant economic impact on small entities of the policies and rules adopted in this First Report and Order, which is found in Appendix B. The Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, will send a copy of the First Report and Order, including the FRFA, to the Chief Counsel for Advocacy of the Small Business Administration.[780]

334. *Initial Regulatory Flexibility Analysis.* As required by the RFA, the Commission has prepared an Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on a substantial number of small entities of the proposals addressed in this Further Notice of Proposed Rulemaking. The IRFA is found in Appendix C. Written public comments are requested on the IRFA. These comments must be filed in accordance with the same filing deadlines for comments on the Further

[774] US Telecom Comments at 8.

[775] Brunner Comments at 30.

[776] JVCKenwood Comments at 11.

[777] Juan Pedro Tomas, *Brazil Gives Final Approval to 5G Tender Process*, RCRWirelessNews (Aug. 21, 2021), https://rcrwireless.com/20210826/business/brazil-gives-final-approval-5g-tender-process.

[778] Juan Pedro Tomas, *Canada to Ban Huawei and ZTE from 5G Networks*, RCRWirelessNews (May 20, 2022), https://rcrwireless.com/20220520/5g/canada-to-ban-huawei-and-zte-from-5g-networks.

[779] *See* 5 U.S.C. § 603.

[780] *See id.* § 603(a). In addition, the *Notice* and RFA (or summaries thereof) will be published in the Federal Register.

Notice, and they should have a separate and distinct heading designating them as responses to the IRFA. The Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, will send a copy of this Further Notice, including the IRFA, to the Chief Counsel for Advocacy of the Small Business Administration, in accordance with the RFA.[781]

335. *Paperwork Reduction Act*. This document contains new or modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law No. 104-13. It will be submitted to the Office of Management and Budget (OMB) for review under section 3507(d) of the PRA. OMB, the general public, and other Federal agencies will be invited to comment on the new or modified information collection requirements contained in this proceeding. In addition, we note that pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, see 44 U.S.C. 3506(c)(4), we previously sought comment on how we might "further reduce the information collection burden for small business concerns with fewer than 25 employees." We have described impacts that might affect small businesses, which includes most businesses with fewer than 25 employees, in the Final Regulatory Flexibility Analysis (FRFA), attached as Appendix B.

336. *Congressional Review Act*. The Commission has determined, and the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget concurs, that this rule is "non-major" under the Congressional Review Act, 5 U.S.C. § 804(2). The Commission will send a copy of this First Report and Order to Congress and the Government Accountability Office pursuant to 5 U.S.C. § 801(a)(1)(A).

337. *Ex Parte Rules – Permit but Disclose.* Pursuant to section 1.1200(a) of the Commission's rules,[782] this Further Notice of Proposed Rulemaking shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules.[783] Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with rule 1.1206(b). In proceedings governed by rule 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (e.g., .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

338. *Comment Period and Filing Procedures.* Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 CFR §§ 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. All filings must refer to ET Docket No. 21-232 or EA Docket No. 21-233.

- Electronic filers: Comments may be filed electronically using the Internet by accessing the Commission's Electronic Comment Filing System (ECFS):

[781] *See id.*

[782] 47 CFR § 1.1200(a).

[783] *Id.* §§ 1.1200 *et seq.*

https://www.fcc.gov/ecfs. *See Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998).

- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing.
    - Filings can be sent by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.
    - Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.
    - U.S. Postal Service first-class, Express, and Priority mail must be addressed to 45 L Street NE, Washington, DC 20554.
- Effective March 19, 2020, and until further notice, the Commission no longer accepts any hand or messenger delivered filings. This is a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19. *See* FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Policy, Public Notice, DA 20-304 (March 19, 2020). https://www.fcc.gov/document/fcc-closes-headquarters-open-window-and-changes-hand-delivery-policy.

339. People with Disabilities: To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (tty).

340. Availability of Documents: Comments, reply comments, and *ex parte* submissions will be publicly available online via ECFS. When the FCC Headquarters reopens to the public, these documents will also be available for public inspection during regular business hours in the FCC Reference Center, Federal Communications Commission, 45 L Street NE, Washington, DC 20554.

341. *Further Information*. For further information, contact Jamie Coleman of the Office of Engineering and Technology, at 202-418-2705 or Jamie.Coleman@fcc.gov.

VII. ORDERING CLAUSES

342. Accordingly, IT IS ORDERED, pursuant to the authority found in sections 4(i), 301, 302, 303, 309(j), 312, 403, and 503 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), 301, 302a, 303, 309(j), 312, 403, 503, and the Secure Equipment Act of 2021, Pub. L. 117-55, 135 Stat. 423, that this Report and Order, Order, and Further Notice of Proposed Rulemaking IS HEREBY ADOPTED.

343. IT IS FURTHER ORDERED that the amendments of parts 2 and 15 of the Commission's rules as set forth in Appendix A ARE ADOPTED, effective on the date of publication in the Federal Register,[784] with the exception of sections 2.903(b), 2.911(d)(5), (6), and (7); 2.929(c); 2.932(e); 2.938(b)(2); 2.1033(b)(1), (2), (3), and (4); 2.1033(c)(1), (2), (3), and (4); 2.1043(b)(2)(i)(B), (C), (D), and (E); and 2.1043(b)(3)(i)(B), (C), (D), and (E), which contain new or modified information collection requirements that require review by the Office of Management and Budget (OMB) under the Paperwork

[784] In accordance with 5 U.S.C. § 553(d), we find good cause to make such rules effective on publication in the Federal Register, in light of the statutory mandate for barring equipment authorizations for specified equipment based on the determination that it "poses an unacceptable risk to the national security of the United States or the security and safety of United States persons." 47 U.S.C. § 1601(b)-(c).

Reduction Act. The Commission directs the Office of Engineering and Technology to establish and announce the effective date of these sections in a document published in the Federal Register after the Commission receives OMB approval.

344. IT IS FURTHER ORDERED that authority is delegated to the Office of Engineering and Technology and the Public Safety and Homeland Security Bureau to develop and inform applicants for equipment authorization, TCBs, and other interested parties with more specific and detailed information on the categories, types, and characteristics of equipment that constitutes "telecommunications equipment" for purposes of the prohibition on future authorization of "covered" equipment identified on the Covered List, and to make such information available on the Commission's website, and to revise that information as appropriate.

345. IT IS FURTHER ORDERED that authority is delegated to the Office of Engineering and Technology and the Public Safety and Homeland Security Bureau to adopt appropriate procedures for streamlined revocation proceedings and to revoke authorizations consistent with the provisions of this Report and Order.

346. IT IS FURTHER ORDERED that the interim freeze shall be effective on release, and authority is delegated to the Office of Engineering and Technology to extend or modify the interim freeze, as appropriate.

347. IT IS FURTHER ORDERED that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this Report and Order, Order, and Further Notice of Proposed Rulemaking, including the Initial and Final Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

348. IT IS FURTHER ORDERED that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this Report and Order, Order, and Further Notice of Proposed Rulemaking, including the Initial and Final Regulatory Flexibility Analysis, to Congress and the Government Accountability Office pursuant to the Congressional Review Act, *see* 5 U.S.C. § 801(a)(1)(A).

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

APPENDIX A

FINAL RULES

For the reasons discussed in the preamble, the Federal Communications Commission amends 47 CFR parts 2 and 15 as follows:

Part 2 — FREQUENCY ALLOCATIONS AND RADIO TREATY MATTERS; GENERAL RULES AND REGULATIONS

1. The authority citation for part 2 continues to read as follows:

Authority: 47 U.S.C. 154, 302a, 303, and 336 unless otherwise noted.

2. Revise § 2.901(a) read as follows:

§ 2.901 Basis and purpose.

(a) In order to carry out its responsibilities under the Communications Act and the various treaties and international regulations, and in order to promote efficient use of the radio spectrum, the Commission has developed technical standards and other requirements for radio frequency equipment and parts or components thereof. The technical standards applicable to individual types of equipment are found in that part of the rules governing the service wherein the equipment is to be operated. In addition to the technical standards provided, the rules governing the service may require that such equipment be authorized under Supplier's Declaration of Conformity or receive a grant of certification from a Telecommunication Certification Body.

* * * * *

3. Add § 2.903 to subpart J to read as follows:

§ 2.903 Prohibition on authorization of equipment on the Covered List.

(a) All equipment on the Covered List, as established pursuant to § 1.50002 of this chapter, is prohibited from obtaining an equipment authorization under this subpart. This includes:

(1) Equipment that would otherwise be subject to certification procedures;

(2) Equipment that would otherwise be subject to Supplier's Declaration of Conformity procedures; and

(3) Equipment that would otherwise be exempt from equipment authorization.

(b) Each entity named on the Covered List as producing covered communications equipment, as established pursuant to § 1.50002 of this chapter, must provide to the Commission the following information: the full name, mailing address or physical address (if different from mailing address), e-mail address, and telephone number of each of that named entity's associated entities (e.g., subsidiaries or affiliates) identified on the Covered List as producing covered communications equipment.

(1) Each entity named on the Covered List as producing covered communications equipment must provide the information described in paragraph (b) of this section no later than [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER];

(2) Each entity named on the Covered List as producing covered communications equipment must provide the information described in paragraph (b) of this section no later than 30 days after the effective date of each updated Covered List; and

(3) Each entity named on the Covered List as producing covered communications equipment must notify the Commission of any changes to the information described in paragraph (b) of this section no later than 30 days after such change occurs.

(c) For purposes of implementing this subpart with regard to the prohibition on authorization of communications equipment on the Covered List, the following definitions apply:

Affiliate. The term "affiliate" means an entity that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another entity; for purposes of this paragraph, the term 'own' means to have, possess, or otherwise control an equity interest (or the equivalent thereof) of more than 10 percent.

Subsidiary. The term "subsidiary" means any entity in which another entity directly or indirectly:

(i) Holds de facto control; or

(ii) Owns or controls more than 50 percent of the outstanding voting stock.

(d) The Commission delegates authority to the Office of Engineering and Technology and the Public Safety and Homeland Security Bureau to develop and provide additional clarifications as appropriate regarding implementation of the prohibition on authorization of covered communications equipment. The Office of Engineering and Technology and Public Safety and Homeland Security Bureau will issue through Public Notice, and publish on the Commission's website, the Commission's relevant guidance on covered communications equipment, as well as further clarifications, and will update and maintain this information as appropriate.

4. Amend § 2.906 by revising paragraph (a) and adding paragraph (d) to read as follows:

§ 2.906 Supplier's Declaration of Conformity.

(a) Supplier's Declaration of Conformity (SDoC) is a procedure where the responsible party, as defined in § 2.909, makes measurements or completes other procedures found acceptable to the Commission to ensure that the equipment complies with the appropriate technical standards and other applicable requirements. Submittal to the Commission of a sample unit or representative data demonstrating compliance is not required unless specifically requested pursuant to § 2.945.

* * * * *

(d) Notwithstanding other parts of this section, equipment otherwise subject to the Supplier's Declaration of Conformity process that is produced by any entity identified on the Covered List, established pursuant to § 1.50002 of this chapter, as producing covered communications equipment is prohibited from obtaining equipment authorization through that process. The rules governing certification apply to authorization of such equipment.

5. Amend § 2.907 by adding paragraph (c) to read as follows:

§ 2.907 Certification.

* * * * *

(c) Any equipment otherwise eligible for authorization pursuant to the Supplier's Declaration of Conformity, or exempt from equipment authorization, produced by any entity identified on the Covered List, established pursuant to § 1.50002 of this chapter, as producing covered communications equipment must obtain equipment authorization through the certification process.

6. Amend § 2.909 by revising paragraph (a) to read as follows:

§ 2.909 Responsible Party.

(a) In the case of equipment that requires the issuance of a grant of certification, the party to whom that grant of certification is issued is responsible for the compliance of the equipment with the applicable technical and other requirements. If any party other than the grantee modifies the radio frequency equipment and that party is not working under the authorization of the grantee pursuant to § 2.929(b), the party performing the modification is responsible for compliance of the product with the applicable administrative and technical provisions in this chapter.

* * * * *

7. Amend § 2.911 by revising paragraph (b) and adding paragraphs (d)(5), (d)(6), and (d)(7) to read as follows:

§ 2.911 Application requirements.

* * * * *

(b) A TCB shall submit an electronic copy of each equipment authorization application to the Commission pursuant to § 2.962(f)(8) on a form prescribed by the Commission at https://www.fcc.gov/eas.

* * * * *

(d) ***

(5) The applicant shall provide a written and signed certification that, as of the date of the filing of the application with a TCB:

(i) The equipment for which the applicant seeks equipment authorization through certification is not prohibited from receiving an equipment authorization pursuant to § 2.903; and

(ii) An affirmative or negative statement as to whether the applicant is identified on the Covered List, established pursuant to § 1.50002 of this chapter, as an entity producing covered communications equipment.

(6) If the Covered List established pursuant to § 1.50002 of this chapter is modified after the date of the written and signed certification required by paragraph (d)(5) of this section but prior to grant of the authorization, then the applicant shall provide a new written and signed certification as required by paragraph (d)(5) of this section.

(7) The applicant shall designate an agent located in the United States for the purpose of accepting service of process on behalf of the applicant.

(i) The applicant shall provide a written certification:

(A) Signed by both the applicant and its designated agent for service of process, if different from the applicant;

(B) Acknowledging the applicant's consent and the designated agent's obligation to accept service of process in the United States for matters related to the applicable equipment, and at the physical U.S. address and e-mail address of its designated agent; and

(C) Acknowledging the applicant's acceptance of its obligation to maintain an agent for service of process in the United States for no less than one year after either the grantee has permanently terminated all marketing and importation of the applicable equipment within the U.S., or the conclusion of any Commission-related administrative or judicial proceeding involving the equipment, whichever is later.

(ii) An applicant located in the United States may designate itself as the agent for service of process.

* * * * *

8. Amend § 2.915 by revising paragraph (a)(1) to read as follows:

§ 2.915 Grant of application.

(a) ***

(1) The equipment is capable of complying with pertinent technical standards of the rule part(s) under which it is to be operated as well as other applicable requirements; and

* * * * *

9. Amend § 2.929 by adding paragraph (b)(3) and revising (c) to read as follows:

§ 2.929 Changes in name, address, ownership or control of grantee.

* * * * *

(b) ***

(3) Such second party must not be an entity identified on the Covered List established pursuant to § 1.50002 of this chapter.

(c) Whenever there is a change in the name and/or address of the grantee of certification, or a change in the name, mailing address or physical address (if different from mailing address), e-mail address, or telephone number of the designated agent for service of process in the United States, notice of such change(s) shall be submitted to the Commission via the Internet at https://www.fcc.gov/eas within 30 days after the beginning use of the new name, mailing address or physical address (if different from mailing address), e-mail address, or telephone number and include:

(1) A written and signed certification that, as of the date of the filing of the notice, the equipment to which the change applies is not prohibited from receiving an equipment authorization pursuant to § 2.903;

(2) An affirmative or negative statement as to whether the applicant is identified on the Covered List, established pursuant to § 1.50002 of this chapter, as an entity producing covered communications equipment; and

(3) The written and signed certifications required under § 2.911(d)(7).

* * * * *

10. Amend § 2.932 by adding paragraph (e) to read as follows:

§ 2.932 Modification of equipment.

* * * * *

(e) All requests for permissive changes shall be accompanied by:

(1) A written and signed certification that, as of the date of the filing of the request for permissive change, the equipment to which the change applies is not prohibited from receiving an equipment authorization pursuant to § 2.903;

(2) An affirmative or negative statement as to whether the applicant is identified on the Covered List, established pursuant to § 1.50002 of this chapter, as an entity producing covered communications equipment; and

(3) The written and signed certifications required under § 2.911(d)(7).

11. Amend § 2.938 by redesignating paragraph (b)(1) through (b)(11) as (b)(1)(i) through (b)(1)(xi) and revising paragraphs (b), (b)(1), and (b)(2) to read as follows:

§ 2.938 Retention of records.

* * * * *

(b) For equipment subject to Supplier's Declaration of Conformity, the responsible party shall, in addition to the requirements in paragraph (a) of this section, maintain the following records:

(1) Measurements made on an appropriate test site that demonstrates compliance with the applicable regulations in this chapter. The record shall:

* * * * *

(2) A written and signed certification that, as of the date of first importation or marketing of the equipment, the equipment for which the responsible party maintains Supplier's Declaration of Conformity is not produced by any entity identified on the Covered List, established pursuant to § 1.50002 of this chapter, as producing covered communications equipment.

* * * * *

12. Amend § 2.939 by revising paragraph (b) and adding paragraph (d) to read as follows:

§ 2.939 Revocation or withdrawal of equipment authorization.

* * * * *

(b) Revocation of an equipment authorization shall be made in the same manner as revocation of radio station licenses, except as provided in paragraph (d) of this section.

* * * * * * * * * *

(d) Notwithstanding other provisions of section 2.939, to the extent a false statement or representation is made in the equipment certification application (see §§ 2.911(d)(5)-(7), 2.932, 2.1033, and 2.1043), or in materials or responses submitted in connection therewith, that the equipment in the subject application is not prohibited from receiving an equipment authorization pursuant to § 2.903, and the equipment certification or modification was granted, if the Commission subsequently determines that the equipment is covered communications equipment, the Commission will revoke such authorization.

(1) If the Office of Engineering and Technology and the Public Safety and Homeland Security Bureau determine that particular authorized equipment is covered communications equipment, and that the certification application for that equipment contained a false statement or representation that the equipment was not covered communications equipment, they will provide written notice to the grantee that a revocation proceeding is being initiated and the grounds under consideration for such revocation.

(2) The grantee will have 10 days in which to respond in writing to the reasons cited for initiating the revocation proceeding. The Office of Engineering and Technology and the Public Safety and Homeland Security Bureau will then review the submissions, request additional information as may be appropriate, and make their determination as to whether to revoke the authorization, providing the reasons for such decision.

13. Amend § 2.1033 by redesignating paragraphs (b)(2) through (b)(14) as paragraphs (b)(5) through (b)(17), revising paragraph (b)(1), adding paragraphs (b)(2), (b)(3), and (b)(4), renumbering paragraphs (c)(2) through (c)(14) as paragraphs (c)(5) through (c)(17), revising paragraph (c)(1), and adding paragraphs (c)(2), (c)(3), and (c)(4) to read as follows:

§ 2.1033 Application for Certification.

* * * * *

(b) ***

(1) The full name, mailing address and physical address (if different from mailing address), email address, and telephone number of:

(i) the applicant for certification; and

(ii) the applicant's agent for service of process in the United States for matters relating to the authorized equipment.

(2) A written and signed certification that, as of, the filing date of the notice, the equipment to which the change applies is not prohibited from receiving an equipment authorization pursuant to § 2.903;

(3) An affirmative or negative statement as to whether the applicant is identified on the Covered List, established pursuant to § 1.50002 of this chapter, as an entity producing covered communications equipment; and

(4) The written and signed certifications required by § 2.911(d)(7).

* * * * *

(c) ***

(1) The full name, mailing address and physical address (if different from mailing address), email address, and telephone number of:

(i) the applicant for certification; and

(ii) the applicant's agent for service of process in the United States for matters relating to the authorized equipment.

(2) A written and signed certification that, as of the filing date of the notice, the equipment to which the change applies is not prohibited from receiving an equipment authorization pursuant to § 2.903.

(3) An affirmative or negative statement as to whether the applicant is identified on the Covered List, established pursuant to § 1.50002 of this chapter, as an entity producing covered communications equipment.

(4) The written and signed certifications required by § 2.911(d)(7).

* * * * *

14. Amend § 2.1043 by revising paragraphs (b)(2) and (b)(3) to read as follows:

§ 2.1043 Changes in certificated equipment.

* * * * *

(b) * * *

(2) A Class II permissive change includes those modifications which degrade the performance characteristics as reported to the Commission at the time of the initial certification. Such degraded performance must still meet the minimum requirements of the applicable rules.

(i) When a Class II permissive change is made by the grantee, the grantee shall provide:

(A) Complete information and the results of tests of the characteristics affected by such change;

(B) A written and signed certification expressly stating that, as of the filing date, the equipment subject to the permissive change is not prohibited from receiving an equipment authorization pursuant to § 2.903;

(C) An affirmative or negative statement as to whether the applicant is identified on the Covered List, established pursuant to § 1.50002 of this chapter, as an entity producing covered communications equipment;

(D) The full name, mailing address and physical address (if different from mailing address), email address, and telephone number of the grantee's designated agent for service of process in the United States for matters relating to the authorized equipment; and

(E) The written and signed certifications required by § 2.911(d)(7).

(ii) The modified equipment shall not be marketed under the existing grant of certification prior to acknowledgement that the change is acceptable.

(3) A Class III permissive change includes modifications to the software of a software defined radio transmitter that change the frequency range, modulation type or maximum output power (either radiated or conducted) outside the parameters previously approved, or that change the circumstances under which the transmitter operates in accordance with Commission rules.

(i) When a Class III permissive change is made, the grantee shall provide:

(A) A description of the changes and test results showing that the equipment complies with the applicable rules with the new software loaded, including compliance with the applicable RF exposure requirements.

(B) A written and signed certification expressly stating that, as of the date of the filing, the equipment subject to the permissive change is not prohibited from receiving an equipment authorization pursuant to § 2.903;

(C) An affirmative or negative statement as to whether the applicant is identified on the Covered List, established pursuant to § 1.50002 of this chapter, as an entity producing covered communications equipment;

(D) The full name, mailing address and physical address (if different from mailing address), email address, and telephone number of the grantee's designated agent for service of process in the United States for matters relating to the authorized equipment; and

(E) The written and signed certifications required by § 2.911(d)(7).

(ii) The modified software shall not be loaded into the equipment, and the equipment shall not be marketed with the modified software under the existing grant of certification, prior to acknowledgement that the change is acceptable.

(iii) Class III changes are permitted only for equipment in which no Class II changes have been made from the originally approved device.

* * * * *

15. Amend § 2.1072 by revising paragraph (a) to read as follows:

§ 2.1072 Limitation on Supplier's Declaration of Conformity.

(a) Supplier's Declaration of Conformity signifies that the responsible party, as defined in § 2.909, has determined that the equipment has been shown to comply with the applicable technical standards and other applicable requirements if no unauthorized change is made in the equipment and if the equipment is properly maintained and operated. Compliance with these standards and other applicable requirements shall not be construed to be a finding by the responsible party with respect to matters not encompassed by the Commission's rules.

* * * * *

Part 15 — RADIOFREQUENCY DEVICES

16. The authority citation for part 15 continues to read as follows:

AUTHORITY: 47 USC 154, 302a, 303, 304, 307, 336, 544a, and 549.

17. Amend § 15.103 by revising the introductory text and adding paragraph (j) to read as follows:

§ 15.103 Exempted devices.

Except as provided in paragraph (j) of this section, the following devices are subject only to the general conditions of operation in §§ 15.5 and 15.29 and are exempt from the specific technical standards and other requirements contained in this part. The operator of the exempted device shall be required to stop operating the device upon a finding by the Commission or its representative that the device is causing harmful interference. Operation shall not resume until the condition causing the harmful interference has been corrected. Although not mandatory, it is strongly recommended that the manufacturer of an exempted device endeavor to have the device meet the specific technical standards in this part.

* * * * *

(j) Notwithstanding other provisions of this section, the rules governing certification apply to any equipment produced by any entity identified on the Covered List, as established pursuant to § 1.50002 of this chapter, as producing covered communications equipment.

* * * * *

APPENDIX B

FINAL REGULATORY FLEXIBILITY ANALYSIS

As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] an Initial Regulatory Flexibility Analysis (IRFA) was incorporated in the *Notice of Proposed Rule Making* (NPRM) in ET Docket No. 21-232.[2] The Commission sought written public comment on the proposals in the *NPRM*,

[1] 5 U.S.C. § 603. The RFA, *see* 5 U.S.C. § 601 – 612, has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[2] *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program,* ET Docket No. 21-232*; Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program*, OEA Docket No. 21-233, Notice of Proposed Rulemaking and Notice of Inquiry, 36 FCC Rcd 10578 (2021).

including comment on the IRFA. This present Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA.[3]

A. Need for, and Objectives of, the Report and Order

1. The Report and Order addresses prohibiting the authorization of any equipment on the list of equipment and services (Covered List) that the Commission maintains pursuant to the Secure and Trusted Communications Networks Act of 2019.[4] The Covered List identifies communications equipment and services that pose an unacceptable risk to the national security of the United States or the security and safety of United States persons.[5] On November 11, 2021, after the close of the comment period, President Biden signed into law the Secure Equipment Act.[6] The Secure Equipment Act requires that, by November 11, 2022, the Commission adopt rules to update "the equipment authorization procedures of the Commission" to "clarify that the Commission will no longer review or approve any application for authorization of equipment that is on the list of covered communications equipment or services" (*i.e.*, the Covered List).[7] The Report and Order fulfills the Commission's statutory mandate in the Secure Equipment Act, prohibiting authorization of any equipment on the Covered List.

B. Summary of Significant Issues Raised by Public Comments in Response to the IRFA

2. There were no comments filed that specifically address the IRFA.

C. Response to Comments by the Chief Counsel for Advocacy of the Small Business Administration

3. Pursuant to the Small Business Jobs Act of 2010, the Commission is required to respond to any comments filed by the Chief Counsel of Advocacy of the Small Business Administration (SBA), and to provide a detailed statement of any change made to the proposed rules as a result of those comments.[8] The Chief Counsel did not file any comments in response to the proposed rules in this proceeding.

D. Description and Estimate of the Number of Small Entities to Which the Rules Will Apply

4. The RFA directs agencies to provide a description of, and where feasible, an estimate of the number of small entities that may be affected by the rules adopted herein.[9] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small

---

[3] *See* 5 U.S.C. § 604.

[4] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601–1609) (Secure Networks Act).

[5] The Commission's Public Safety and Homeland Security Bureau maintains the list at on the Commission's website at https://www.fcc.gov/supplychain/coveredlist.

[6] Secure Equipment Act of 2021, Pub. L. No. 117-55, 135 Stat. 423 (2021) (codified at 47 U.S.C. § 1601 (Statutory Notes and Related Subsidiaries)) (Secure Equipment Act).

[7] Secure Equipment Act, §§ 2(a)(1)-(2). The Covered List is posted on the Commission's website at https://www.fcc.gov/supplychain/coveredlist.

The Secure Equipment Act also includes other provisions. In particular, the Commission may not provide for review or revocation of any equipment authorization granted before the date on which it adopts rules to prohibit approval of authorization of equipment on the Covered List; the Commission is not, however, not prohibited from examining the necessity of review or revocation of any equipment authorization on the basis of the equipment being on the Covered List or adopting rules providing for any such review or revocation. Secure Equipment Act, §§ 3(A), 3(B)(i)-(ii).

[8] 5 U.S.C. § 604 (a)(3).

[9] *Id.*

organization," and "small governmental jurisdiction."[10] In addition, the term "small business" has the same meaning has the term "small business concern" under the Small Business Act.[11] A "small business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.[12]

5. ***Small Businesses, Small Organizations, Small Governmental Jurisdictions.*** Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe, at the outset, three broad groups of small entities that could be directly affected herein.[13] First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the Small Business Administration's (SBA) Office of Advocacy, in general a small business is an independent business having fewer than 500 employees.[14] These types of small businesses represent 99.9% of all businesses in the United States, which translates to 32.5 million businesses.[15]

6. Next, the type of small entity described as a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field."[16] The Internal Revenue Service (IRS) uses a revenue benchmark of $50,000 or less to delineate its annual electronic filing requirements for small exempt organizations.[17] Nationwide, for tax year 2020, there were approximately 447,689 small exempt organizations in the U.S. reporting revenues of $50,000 or less according to the registration and tax data for exempt organizations available from the IRS.[18]

7. Finally, the small entity described as a "small governmental jurisdiction" is defined generally as "governments of cities, counties, towns, townships, villages, school districts, or special

---

[10] 5 U.S.C. § 601(6).

[11] 5 U.S.C. § 601(3) (incorporating by reference the definition of "small-business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register."

[12] 15 U.S.C. § 632.

[13] *See* 5 U.S.C. § 601(3)-(6).

[14] *See* SBA, Office of Advocacy, Frequently Asked Questions, "What is a small business?," https://cdn.advocacy.sba.gov/wp-content/uploads/2021/11/03093005/Small-Business-FAQ-2021.pdf. (Nov 2021).

[15] *Id*.

[16] *See* 5 U.S.C. § 601(4).

[17] The IRS benchmark is similar to the population of less than 50,000 benchmark in 5 U.S.C § 601(5) that is used to define a small governmental jurisdiction. Therefore, the IRS benchmark has been used to estimate the number small organizations in this small entity description. S*ee* Annual Electronic Filing Requirement for Small Exempt Organizations – Form 990-N (e-Postcard), "Who must file,"

https://www.irs.gov/charities-non-profits/annual-electronic-filing-requirement-for-small-exempt-organizations-form-990-n-e-postcard. We note that the IRS data does not provide information on whether a small exempt organization is independently owned and operated or dominant in its field.

[18] *See* Exempt Organizations Business Master File Extract (EO BMF), "CSV Files by Region," https://www.irs.gov/charities-non-profits/exempt-organizations-business-master-file-extract-eo-bmf. The IRS Exempt Organization Business Master File (EO BMF) Extract provides information on all registered tax-exempt/non-profit organizations. The data utilized for purposes of this description was extracted from the IRS EO BMF data for businesses for the tax year 2020 with revenue less than or equal to $50,000 for Region 1-Northeast Area (58,577), Region 2-Mid-Atlantic and Great Lakes Areas (175,272), and Region 3-Gulf Coast and Pacific Coast Areas (213,840) that includes the continental U.S., Alaska, and Hawaii. This data does not include information for Puerto Rico.

districts, with a population of less than fifty thousand."[19] U.S. Census Bureau data from the 2017 Census of Governments[20] indicate there were 90,075 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States.[21] Of this number, there were 36,931 general purpose governments (county,[22] municipal, and town or township[23]) with populations of less than 50,000 and 12,040 special purpose governments—independent school districts[24] with enrollment populations of less than 50,000.[25] Accordingly, based on the 2017 U.S. Census of Governments data, we estimate that at least 48,971 entities fall into the category of "small governmental jurisdictions."[26]

8. ***Satellite Telecommunications.*** This industry comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications."[27] Satellite telecommunications service providers include satellite and earth station operators. The SBA small business size standard for this industry classifies a business with $38.5 million or less in annual receipts as small.[28] U.S. Census Bureau data for 2017 show that 275 firms in this industry operated for the entire year.[29] Of this number, 242 firms had revenue of less than

[19] *See* 5 U.S.C. § 601(5).

[20] *See* 13 U.S.C. § 161. The Census of Governments survey is conducted every five (5) years compiling data for years ending with "2" and "7." *See also* Census of Governments, https://www.census.gov/programs-surveys/cog/about.html.

[21] *See* U.S. Census Bureau, 2017 Census of Governments – Organization Table 2. Local Governments by Type and State: 2017 [CG1700ORG02], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. Local governmental jurisdictions are made up of general purpose governments (county, municipal and town or township) and special purpose governments (special districts and independent school districts). *See also* tbl.2. CG1700ORG02 Table Notes Local Governments by Type and State_2017.

[22] *See id.* at tbl.5. County Governments by Population-Size Group and State: 2017 [CG1700ORG05], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 2,105 county governments with populations less than 50,000. This category does not include subcounty (municipal and township) governments.

[23] *See id.* at tbl.6. Subcounty General-Purpose Governments by Population-Size Group and State: 2017 [CG1700ORG06], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 18,729 municipal and 16,097 town and township governments with populations less than 50,000.

[24] *See id.* at tbl.10. Elementary and Secondary School Systems by Enrollment-Size Group and State: 2017 [CG1700ORG10], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 12,040 independent school districts with enrollment populations less than 50,000. *See also* tbl.4. Special-Purpose Local Governments by State Census Years 1942 to 2017 [CG1700ORG04], CG1700ORG04 Table Notes_Special Purpose Local Governments by State Census Years 1942 to 2017.

[25] While the special purpose governments category also includes local special district governments, the 2017 Census of Governments data does not provide data aggregated based on population size for the special purpose governments category. Therefore, only data from independent school districts is included in the special purpose governments category.

[26] This total is derived from the sum of the number of general purpose governments (county, municipal and town or township) with populations of less than 50,000 (36,931) and the number of special purpose governments - independent school districts with enrollment populations of less than 50,000 (12,040), from the 2017 Census of Governments - Organizations tbls.5, 6 & 10.

[27] *See* U.S. Census Bureau, *2017 NAICS Definition, "517410 Satellite Telecommunications,"* https://www.census.gov/naics/?input=517410&year=2017&details=517410.

[28] *See* 13 CFR § 121.201, NAICS Code 517410.

[29] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 517410,

(continued….)

$25 million.[30] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 71 providers that reported they were engaged in the provision of satellite telecommunications services.[31] Of these providers, the Commission estimates that approximately 48 providers have 1,500 or fewer employees.[32] Consequently using the SBA's small business size standard, a little more than of these providers can be considered small entities.

9. ***All Other Telecommunications.*** This industry is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation.[33] This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems.[34] Providers of Internet services (e.g. dial-up ISPs) or voice over Internet protocol (VoIP) services, via client-supplied telecommunications connections are also included in this industry.[35] The SBA small business size standard for this industry classifies firms with annual receipts of $35 million or less as small.[36] U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year.[37] Of those firms, 1,039 had revenue of less than $25 million.[38] Based on this data, the Commission estimates that the majority of "All Other Telecommunications" firms can be considered small.

10. ***Fixed Satellite Transmit/Receive Earth Stations.*** There are approximately 4,303 earth station authorizations, a portion of which are Fixed Satellite Transmit/Receive Earth Stations. We do not request nor collect annual revenue information and are unable to estimate the number of the earth stations that would constitute a small business under the SBA definition. However, the majority of these stations could be impacted by our proposed rules.

11. ***Fixed Satellite Small Transmit/Receive Earth Stations***. Neither the SBA nor the Commission have developed a small business size standard specifically applicable to Fixed Satellite Small Transmit/Receive Earth Stations. Satellite Telecommunications[39] is the closest industry with an

---

https://data.census.gov/cedsci/table?y=2017&n=517410&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[30] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[31] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[32] *Id.*

[33] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517919 All Other Telecommunications,*" https://www.census.gov/naics/?input=517919&year=2017&details=517919.

[34] *Id.*

[35] *Id*.

[36] *See* 13 CFR § 121.201, NAICS Code 517919.

[37] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 517919, https://data.census.gov/cedsci/table?y=2017&n=517919&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[38] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[39] *See* U.S. Census Bureau, *2017 NAICS Definition, "517410 Satellite Telecommunications,"* https://www.census.gov/naics/?input=517410&year=2017&details=517410.

SBA small business size standard. The SBA size standard for this industry classifies a business as small if it has $35 million or less in annual receipts.[40] For this industry, U.S. Census Bureau data for 2017 show that there were a total of 275 firms that operated for the entire year.[41] Of this total, 242 firms had revenue of less than $25 million.[42] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 71 providers that reported they were engaged in the provision of satellite telecommunications services.[43] Of these providers, the Commission estimates that approximately 48 providers have 1,500 or fewer employees.[44] Consequently using the SBA's small business size standard, a little more than half of these providers can be considered small entities.

12. ***Mobile Satellite Earth Stations.*** Neither the SBA nor the Commission have developed a small business size standard specifically applicable to Mobile Satellite Earth Stations. Satellite Telecommunications[45] is the closest industry with an SBA small business size standard. The SBA small business size standard classifies a business with $35 million or less in annual receipts as small.[46] For this industry, U.S. Census Bureau data for 2017 show that there were 275 firms that operated for the entire year.[47] Of this number, 242 firms had revenue of less than $25 million.[48] Thus, for this industry under the SBA size standard, the Commission estimates that the majority of Mobile Satellite Earth Station licensees are small entities. Additionally, based on Commission data as of December 17, 2021, there were 5 Mobile Satellite Earth Stations licensees.[49] The Commission does not request nor collect annual revenue information and is therefore unable to estimate the number of mobile satellite earth stations that would be classified as a small business under the SBA size standard.

13. ***Wireless Telecommunications Carriers (except Satellite).*** This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide

[40] *See* 13 CFR § 121.201, NAICS Code 517410.

[41] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 517410, https://data.census.gov/cedsci/table?y=2017&n=517410&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[42] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[43] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[44] *Id.*

[45] *See* U.S. Census Bureau, *2017 NAICS Definition, "517410 Satellite Telecommunications,"* https://www.census.gov/naics/?input=517410&year=2017&details=517410.

[46] *See* 13 CFR § 121.201, NAICS Code 517410.

[47] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 517410, https://data.census.gov/cedsci/table?y=2017&n=517410&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[48] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[49] Based on a FCC International Bureau, *MyIBFS* System, Advanced Search on December 17, 2021, https://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr030b.hts?set=. Search Terms used - Nature of Application Service = SES - Satellite Earth Station; Application Type = LIC – License; Class of Station = MES – Mobile Earth Station; and under "Filing Status" = Current.

communications via the airwaves.[50] Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless internet access, and wireless video services.[51] The SBA size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[52] U.S. Census Bureau data for 2017 show that there were 2,893 firms in this industry that operated for the entire year.[53] Of that number, 2,837 firms employed fewer than 250 employees.[54] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 797 providers that reported they were engaged in the provision of wireless services.[55] Of these providers, the Commission estimates that 715 providers have 1,500 or fewer employees.[56] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

14. ***Wireless Carriers and Service Providers.*** Wireless Telecommunications Carriers (*except* Satellite) is the closest industry with an SBA small business size standard applicable to these service providers.[57] The SBA small business size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[58] U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year.[59] Of this number, 2,837 firms employed fewer than 250 employees.[60] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 797 providers that reported they were engaged in the provision of wireless services.[61] Of these providers, the Commission estimates that 715 providers have 1,500 or fewer employees.[62] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities. *Wireless Carriers and Service Providers*. Wireless Telecommunications Carriers (*except* Satellite) is the closest industry with an SBA small business size standard applicable to

---

[50] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite),"* https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[51] *Id.*

[52] *See* 13 CFR § 121.201, NAICS Code 517312.

[53] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[54] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[55] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[56] *Id.*

[57] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers* (*except Satellite*)," https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[58] *See* 13 CFR § 121.201, NAICS Code 517312.

[59] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[60] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[61] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[62] *Id.*

these service providers.[63] The SBA small business size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[64] U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year.[65] Of this number, 2,837 firms employed fewer than 250 employees.[66] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 797 providers that reported they were engaged in the provision of wireless services.[67] Of these providers, the Commission estimates that 715 providers have 1,500 or fewer employees.[68] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

15. ***Wired Telecommunications Carriers.*** The U.S. Census Bureau defines this industry as establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks.[69] Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services.[70] By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry.[71] Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.[72]

16. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[73] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[74] Of this number, 2,964 firms operated

---

[63] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers* (*except Satellite*)," https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[64] *See* 13 CFR § 121.201, NAICS Code 517312.

[65] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[66] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[67] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[68] *Id.*

[69] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[70] *Id.*

[71] *Id.*

[72] Fixed Local Service Providers include the following types of providers: Incumbent Local Exchange Carriers (ILECs), Competitive Access Providers (CAPs) and Competitive Local Exchange Carriers (CLECs), Cable/Coax CLECs, Interconnected VOIP Providers, Non-Interconnected VOIP Providers, Shared-Tenant Service Providers, Audio Bridge Service Providers, and Other Local Service Providers. Local Resellers fall into another U.S. Census Bureau industry group and therefore data for these providers is not included in this industry.

[73] *See* 13 CFR § 121.201, NAICS Code 517311.

[74] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

with fewer than 250 employees.[75] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 5,183 providers that reported they were engaged in the provision of fixed local services.[76] Of these providers, the Commission estimates that 4,737 providers have 1,500 or fewer employees.[77] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities. *Licenses Assigned by Auctions.* The Commission's small business size standards with respect to Licenses Assigned by Auction involve eligibility for bidding credits and installment payments in the auction of licenses for various wireless frequencies. In the auction of these licenses, the Commission may define and adopt criteria for different classes small businesses – very small, small or entrepreneur. The criteria for these small business classes may be statutorily defined in the Commission's rules[78] or may require consultation with the U.S. Small Business Administration, Office of Size Standards.[79] For licenses subject to auction, the number of winning bidders that qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in service. In addition, the Commission does not generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated.

17. *Private Land Mobile Radio Licensees*. Private land mobile radio (PLMR) systems serve an essential role in a vast range of industrial, business, land transportation, and public safety activities. Companies of all sizes operating in all U.S. business categories use these radios. Wireless Telecommunications Carriers (*except* Satellite)[80] which encompasses business entities engag*ed in radiotelephone communications,* is the closest industry with an SBA small business size standard applicable to these services. The SBA small size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[81] U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year.[82] Of this number, 2,837 firms employed fewer than 250 employees.[83] Thus under the SBA size standard, the Commission estimates licensees in this industry can be considered small.

[75] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[76] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[77] *Id.*

[78] *See* 47 CFR § 27.702(a)(1)-(3). This is an illustrative example of three types of small businesses for an auction of licenses in a certain frequency that is codified in the Commission's rules.

[79] *See* 5 U.S.C. § 601(3).

[80] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite),"* https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[81] *See* 13 CFR § 121.201, NAICS Code 517312.

[82] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[83] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

18. Based on Commission data as of December 14, 2021, there are approximately 387,370 active PLMR licenses.[84] Active PLMR licenses include 3,577 licenses in the 4.9 GHz band;[85] 19,011 licenses in the 800 MHz band;[86] and 2,716 licenses in the 900 MHz band.[87] Since the Commission does not collect data on the number of employees for licensees providing these services, at this time we are not able to estimate the number of licensees with active licenses that would qualify as small under the SBA's small business size standard. Nevertheless, the Commission believes that a substantial number of PLMR licensees are small entities.

19. ***Private Land Mobile Radio Licensees***. Private land mobile radio (PLMR) systems serve an essential role in a vast range of industrial, business, land transportation, and public safety activities. Companies of all sizes operating in all U.S. business categories use these radios.

20. ***Wireless Telecommunications Carriers (except Satellite)*** [88] which encompasses business entities engag*ed in radiotelephone communications,* is the closest industry with an SBA small business size standard applicable to these services. The SBA small size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[89] U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year.[90] Of this number, 2,837 firms employed fewer than 250 employees.[91] Thus under the SBA size standard, the Commission estimates licensees in this industry can be considered small.

---

[84] Based on a FCC Universal Licensing System search on December 14, 2021, https://wireless2.fcc.gov/UlsApp/UlsSearch/searchAdvanced.jsp. Search parameters: Service Group = All, "Match only the following radio service(s)", Radio Service = GB, GE, GF, GI, GJ, GO, GP, GU, IG, IQ, PA, PW, QM, QQ, RS, SG, SL, SP, SY, YB, YE, YF, YG, YI, YJ, YO, YP, YU, YW; Authorization Type = All; Status = Active. We note that the number of active licenses does not equate to the number of licensees. A licensee can have one or more licenses.

[85] Based on a FCC Universal Licensing System search on December 14, 2021, https://wireless2.fcc.gov/UlsApp/UlsSearch/searchAdvanced.jsp. Search parameters: Service Group = All, "Match only the following radio service(s)", Radio Service = PA; Authorization Type = All; Status = Active. We note that the number of active licenses does not equate to the number of licensees. A licensee can have one or more licenses.

[86] Based on a FCC Universal Licensing System search on December 14, 2021, https://wireless2.fcc.gov/UlsApp/UlsSearch/searchAdvanced.jsp. Search parameters: Service Group = All, "Match only the following radio service(s)", Radio Service = GB, GE, GF, GJ, GM, GO, GP, YB, YE, YF, YJ, YM, YO, YP, YX; Authorization Type = All; Status = Active. We note that the number of active licenses does not equate to the number of licensees. A licensee can have one or more licenses.

[87] Based on a FCC Universal Licensing System search on December 14, 2021, https://wireless2.fcc.gov/UlsApp/UlsSearch/searchAdvanced.jsp. Search parameters: Service Group = All, "Match only the following radio service(s)", Radio Service = GI, GR, GU, YD, YS, YU; Authorization Type = All; Status = Active. We note that the number of active licenses does not equate to the number of licensees. A licensee can have one or more licenses.

[88] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite),"* https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[89] *See* 13 CFR § 121.201, NAICS Code 517312.

[90] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[91] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

21. Based on Commission data as of December 14, 2021, there are approximately 387,370 active PLMR licenses.[92] Active PLMR licenses include 3,577 licenses in the 4.9 GHz band;[93] 19,011 licenses in the 800 MHz band;[94] and 2,716 licenses in the 900 MHz band.[95] Since the Commission does not collect data on the number of employees for licensees providing these services, at this time we are not able to estimate the number of licensees with active licenses that would qualify as small under the SBA's small business size standard. Nevertheless, the Commission believes that a substantial number of PLMR licensees are small entities.

22. ***Fixed Microwave Services.*** Fixed microwave services include common carrier,[96] private-operational fixed,[97] and broadcast auxiliary radio services.[98] They also include the Upper Microwave Flexible Use Service (UMFUS),[99] Millimeter Wave Service (70/80/90 GHz),[100] Local Multipoint Distribution Service (LMDS),[101] the Digital Electronic Message Service (DEMS),[102] 24 GHz Service,[103] Multiple Address Systems (MAS),[104] and Multichannel Video Distribution and Data Service

[92] Based on a FCC Universal Licensing System search on December 14, 2021, https://wireless2.fcc.gov/UlsApp/UlsSearch/searchAdvanced.jsp. Search parameters: Service Group = All, "Match only the following radio service(s)", Radio Service = GB, GE, GF, GI, GJ, GO, GP, GU, IG, IQ, PA, PW, QM, QQ, RS, SG, SL, SP, SY, YB, YE, YF, YG, YI, YJ, YO, YP, YU, YW; Authorization Type = All; Status = Active. We note that the number of active licenses does not equate to the number of licensees. A licensee can have one or more licenses.

[93] Based on a FCC Universal Licensing System search on December 14, 2021, https://wireless2.fcc.gov/UlsApp/UlsSearch/searchAdvanced.jsp. Search parameters: Service Group = All, "Match only the following radio service(s)", Radio Service = PA; Authorization Type = All; Status = Active. We note that the number of active licenses does not equate to the number of licensees. A licensee can have one or more licenses.

[94] Based on a FCC Universal Licensing System search on December 14, 2021, https://wireless2.fcc.gov/UlsApp/UlsSearch/searchAdvanced.jsp. Search parameters: Service Group = All, "Match only the following radio service(s)", Radio Service = GB, GE, GF, GJ, GM, GO, GP, YB, YE, YF, YJ, YM, YO, YP, YX; Authorization Type = All; Status = Active. We note that the number of active licenses does not equate to the number of licensees. A licensee can have one or more licenses.

[95] Based on a FCC Universal Licensing System search on December 14, 2021, https://wireless2.fcc.gov/UlsApp/UlsSearch/searchAdvanced.jsp. Search parameters: Service Group = All, "Match only the following radio service(s)", Radio Service = GI, GR, GU, YD, YS, YU; Authorization Type = All; Status = Active. We note that the number of active licenses does not equate to the number of licensees. A licensee can have one or more licenses.

[96] *See* 47 CFR part 101, subparts C and I.

[97] *See id*. subparts C and H.

[98] Auxiliary Microwave Service is governed by part 74 of Title 47 of the Commission's Rules. *See* 47 CFR part 74. Available to licensees of broadcast stations and to broadcast and cable network entities, broadcast auxiliary microwave stations are used for relaying broadcast television signals from the studio to the transmitter, or between two points such as a main studio and an auxiliary studio. The service also includes mobile TV pickups, which relay signals from a remote location back to the studio.

[99] *See* 47 CFR part 30.

[100] *See* 47 CFR part 101, subpart Q.

[101] *See id*. subpart L.

[102] *See id*. subpart G.

[103] *See id*.

[104] *See id.* subpart O.

(MVDDS),[105] where in some bands licensees can choose between common carrier and non-common carrier status.[106] Wireless Telecommunications Carriers (*except* Satellite)[107] is the closest industry with an SBA small business size standard applicable to these services. The SBA small size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[108] U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year.[109] Of this number, 2,837 firms employed fewer than 250 employees.[110] Thus under the SBA size standard, the Commission estimates that a majority of fixed microwave service licensees can be considered small.

23. The Commission's small business size standards with respect to fixed microwave services involve eligibility for bidding credits and installment payments in the auction of licenses for the various frequency bands included in fixed microwave services. When bidding credits are adopted for the auction of licenses in fixed microwave services frequency bands, such credits may be available to several types of small businesses based average gross revenues (small, very small and entrepreneur) pursuant to the competitive bidding rules adopted in conjunction with the requirements for the auction and/or as identified in part 101 of the Commission's rules for the specific fixed microwave services frequency bands.[111]

24. ***Other Communications Equipment Manufacturing.*** This industry comprises establishments primarily engaged in manufacturing communications equipment (except telephone apparatus, and radio and television broadcast, and wireless communications equipment).[112] Examples of such manufacturing include fire detection and alarm systems manufacturing, Intercom systems and equipment manufacturing, and signals (e.g., highway, pedestrian, railway, traffic) manufacturing.[113] The SBA small business size standard for this industry classifies firms having 750 or fewer employees as small.[114] For this industry, U.S. Census Bureau data for 2017 shows that 321 firms operated for the entire year.[115] Of that number, 310 firms operated with fewer than 250 employees.[116] Based on this data, we conclude that the majority of Other Communications Equipment Manufacturers are small.

---

[105] *See id*. subpart P.

[106] *See* 47 CFR §§ 101.533, 101.1017.

[107] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers* (*except Satellite*)," https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[108] *See* 13 CFR § 121.201, NAICS Code 517312.

[109] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[110] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[111] *See* 47 CFR §§ 101.538(a)(1)-(3), 101.1112(b)-(d), 101.1319(a)(1)-(2), and 101.1429(a)(1)-(3).

[112] *See* U.S. Census Bureau, *2017 NAICS Definitions, "334290 Other Communications Equipment Manufacturing,*" https://www.census.gov/naics/?input=334290&year=2017&details=334290.

[113] *Id.*

[114] *See* 13 CFR 121.201, NAICS Code 334290.

[115] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 334290, https://data.census.gov/cedsci/table?y=2017&n=334290&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[116] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

25. ***Fixed Microwave Services.*** Fixed microwave services include common carrier,[117] private-operational fixed,[118] and broadcast auxiliary radio services.[119] They also include the Upper Microwave Flexible Use Service (UMFUS),[120] Millimeter Wave Service (70/80/90 GHz),[121] Local Multipoint Distribution Service (LMDS),[122] the Digital Electronic Message Service (DEMS),[123] 24 GHz Service,[124] Multiple Address Systems (MAS),[125] and Multichannel Video Distribution and Data Service (MVDDS),[126] where in some bands licensees can choose between common carrier and non-common carrier status.[127] Wireless Telecommunications Carriers (*except* Satellite)[128] is the closest industry with an SBA small business size standard applicable to these services. The SBA small size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[129] U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year.[130] Of this number, 2,837 firms employed fewer than 250 employees.[131] Thus under the SBA size standard, the Commission estimates that a majority of fixed microwave service licensees can be considered small.

26. The Commission's small business size standards with respect to fixed microwave services involve eligibility for bidding credits and installment payments in the auction of licenses for the various frequency bands included in fixed microwave services. When bidding credits are adopted for the auction of licenses in fixed microwave services frequency bands, such credits may be available to several types of small businesses based average gross revenues (small, very small and entrepreneur) pursuant to the competitive bidding rules adopted in conjunction with the requirements for the auction and/or as identified in part 101 of the Commission's rules for the specific fixed microwave services frequency bands.[132] In frequency bands where licenses were subject to auction, the Commission notes that as a general matter, the number of winning bidders that qualify as small businesses at the close of an auction

---

[117] *See* 47 CFR part 101, subparts C and I.

[118] *See id*. subparts C and H.

[119] Auxiliary Microwave Service is governed by part 74 of Title 47 of the Commission's Rules. *See* 47 CFR part 74. Available to licensees of broadcast stations and to broadcast and cable network entities, broadcast auxiliary microwave stations are used for relaying broadcast television signals from the studio to the transmitter, or between two points such as a main studio and an auxiliary studio. The service also includes mobile TV pickups, which relay signals from a remote location back to the studio.

[120] *See* 47 CFR part 30.

[121] *See* 47 CFR part 101, subpart Q.

[122] *See id*. subpart L.

[123] *See id*. subpart G.

[124] *See id*.

[125] *See id.* subpart O.

[126] *See id*. subpart P.

[127] *See* 47 CFR §§ 101.533, 101.1017.

[128] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers* (*except Satellite*)," https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[129] *See* 13 CFR § 121.201, NAICS Code 517312.

[130] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[131] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[132] *See* 47 CFR §§ 101.538(a)(1)-(3), 101.1112(b)-(d), 101.1319(a)(1)-(2), and 101.1429(a)(1)-(3).

does not necessarily represent the number of small businesses currently in service. Further, the Commission does not generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated. Additionally, since the Commission does not collect data on the number of employees for licensees providing these services, at this time we are not able to estimate the number of licensees with active licenses that would qualify as small under the SBA's small business size standard.

27. ***License Assigned by Auctions.*** The Commission's small business size standards with respect to Licenses Assigned by Auction involve eligibility for bidding credits and installment payments in the auction of licenses for various wireless frequencies. In the auction of these licenses, the Commission may define and adopt criteria for different classes small businesses – very small, small or entrepreneur. The criteria for these small business classes may be statutorily defined in the Commission's rules[133] or may require consultation with the U.S. Small Business Administration, Office of Size Standards.[134] For licenses subject to auction, the number of winning bidders that qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in service. In addition, the Commission does not generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated. *Private Land Mobile Radio Licensees*. Private land mobile radio (PLMR) systems serve an essential role in a vast range of industrial, business, land transportation, and public safety activities. Companies of all sizes operating in all U.S. business categories use these radios. Wireless Telecommunications Carriers (*except* Satellite)[135] which encompasses business entities engaged *in radiotelephone communications,* is the closest industry with an SBA small business size standard applicable to these services. The SBA small size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[136] U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year.[137] Of this number, 2,837 firms employed fewer than 250 employees.[138] Thus under the SBA size standard, the Commission estimates licensees in this industry can be considered small.

28. Based on Commission data as of December 14, 2021, there are approximately 387,370 active PLMR licenses.[139] Active PLMR licenses include 3,577 licenses in the 4.9 GHz band;[140] 19,011

---

[133] *See* 47 CFR § 27.702(a)(1)-(3). This is an illustrative example of three types of small businesses for an auction of licenses in a certain frequency that is codified in the Commission's rules.

[134] *See* 5 U.S.C. § 601(3).

[135] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite),"* https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[136] *See* 13 CFR § 121.201, NAICS Code 517312.

[137] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[138] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[139] Based on a FCC Universal Licensing System search on December 14, 2021, https://wireless2.fcc.gov/UlsApp/UlsSearch/searchAdvanced.jsp. Search parameters: Service Group = All, "Match only the following radio service(s)", Radio Service = GB, GE, GF, GI, GJ, GO, GP, GU, IG, IQ, PA, PW, QM, QQ, RS, SG, SL, SP, SY, YB, YE, YF, YG, YI, YJ, YO, YP, YU, YW; Authorization Type = All; Status = Active. We note that the number of active licenses does not equate to the number of licensees. A licensee can have one or more licenses.

[140] Based on a FCC Universal Licensing System search on December 14, 2021, https://wireless2.fcc.gov/UlsApp/UlsSearch/searchAdvanced.jsp. Search parameters: Service Group = All, "Match only the following radio service(s)", Radio Service = PA; Authorization Type = All; Status = Active. We note that the number of active licenses does not equate to the number of licensees. A licensee can have one or more licenses.

licenses in the 800 MHz band;[141] and 2,716 licenses in the 900 MHz band.[142] Since the Commission does not collect data on the number of employees for licensees providing these services, at this time we are not able to estimate the number of licensees with active licenses that would qualify as small under the SBA's small business size standard. Nevertheless, the Commission believes that a substantial number of PLMR licensees are small entities.

29. ***Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing.*** This industry comprises establishments primarily engaged in manufacturing radio and television broadcast and wireless communications equipment.[143] Examples of products made by these establishments are: transmitting and receiving antennas, cable television equipment, GPS equipment, pagers, cellular phones, mobile communications equipment, and radio and television studio and broadcasting equipment.[144] The SBA small business size standard for this industry classifies businesses having 1,250 employees or less as small.[145] U.S. Census Bureau data for 2017 show that there were 656 firms in this industry that operated for the entire year.[146] Of this number, 624 firms had fewer than 250 employees.[147] Thus, under the SBA size standard, the majority of firms in this industry can be considered small.

30. ***Auxiliary, Special Broadcast and Other Program Distribution Services.*** This service involves a variety of transmitters, generally used to relay broadcast programming to the public (through translator and booster stations) or within the program distribution chain (from a remote news gathering unit back to the station). Neither the SBA nor the Commission have developed a small business size standard applicable to broadcast auxiliary licensees. The closest applicable industries with an SBA small business size standard fall within two industries - Radio Stations[148] and Television Broadcasting.[149] The SBA small business size standard for Radio Stations classifies firms having $41.5 million or less in

---

[141] Based on a FCC Universal Licensing System search on December 14, 2021, https://wireless2.fcc.gov/UlsApp/UlsSearch/searchAdvanced.jsp. Search parameters: Service Group = All, "Match only the following radio service(s)", Radio Service = GB, GE, GF, GJ, GM, GO, GP, YB, YE, YF, YJ, YM, YO, YP, YX; Authorization Type = All; Status = Active. We note that the number of active licenses does not equate to the number of licensees. A licensee can have one or more licenses.

[142] Based on a FCC Universal Licensing System search on December 14, 2021, https://wireless2.fcc.gov/UlsApp/UlsSearch/searchAdvanced.jsp. Search parameters: Service Group = All, "Match only the following radio service(s)", Radio Service = GI, GR, GU, YD, YS, YU; Authorization Type = All; Status = Active. We note that the number of active licenses does not equate to the number of licensees. A licensee can have one or more licenses.

[143] *See* U.S. Census Bureau, *2017 NAICS Definition, "334220 Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing,"* https://www.census.gov/naics/?input=334220&year=2017&details=334220.

[144] *Id*.

[145] *See* 13 CFR § 121.201, NAICS Code 334220.

[146] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 334220, https://data.census.gov/cedsci/table?y=2017&n=334220&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[147] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[148] *See* U.S. Census Bureau, *2017 NAICS Definition, "515112 Radio Stations*," https://www.census.gov/naics/?input=515112&year=2017&details=515112.

[149] *See* U.S. Census Bureau, *2017 NAICS Definition, "515120 Television Broadcasting,"* https://www.census.gov/naics/?input=515120&year=2017&details=515120.

annual receipts as small.[150] U.S. Census Bureau data for 2017 show that 2,963 firms operated in this industry during that year.[151] Of that number, 1,879 firms operated with revenue of less than $25 million per year.[152] For Television Broadcasting, the SBA small business size standard also classifies firms having $41.5 million or less in annual receipts as small.[153] U.S. Census Bureau data for 2017 show that 744 firms in this industry operated for the entire year.[154] Of that number, 657 firms had revenue of less than $25 million per year.[155] Accordingly, based on the U.S. Census Bureau data for Radio Stations and Television Broadcasting, the Commission estimates that the majority of Auxiliary, Special Broadcast and Other Program Distribution Services firms are small under the SBA size standard.

31. ***Radio Frequency Equipment Manufacturers (RF Manufacturers).*** There are several analogous industries with an SBA small business size standard that are applicable to RF Manufacturers. These industries are Fixed Microwave Services, Other Communications Equipment Manufacturing, and Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing. A description of these industries and the SBA small business size standards are detailed below.

32. ***Other Communications Equipment Manufacturing.*** This industry comprises establishments primarily engaged in manufacturing communications equipment (except telephone apparatus, and radio and television broadcast, and wireless communications equipment).[156] Examples of such manufacturing include fire detection and alarm systems manufacturing, Intercom systems and equipment manufacturing, and signals (e.g., highway, pedestrian, railway, traffic) manufacturing.[157] The SBA small business size standard for this industry classifies firms having 750 or fewer employees as small.[158] For this industry, U.S. Census Bureau data for 2017 shows that 321 firms operated for the entire

[150] *See* 13 CFR § 121.201, NAICS Code 515112.

[151] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 515112, https://data.census.gov/cedsci/table?y=2017&n=515112&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false. We note that the US Census Bureau withheld publication of the number of firms that operated for the entire year.

[152] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We note that the U.S. Census Bureau withheld publication of the number of firms that operated with sales/value of shipments/revenue in the individual categories for less than $100,000, and $100,000 to $249,999 to avoid disclosing data for individual companies (see Cell Notes for the sales/value of shipments/revenue in these categories). Therefore, the number of firms with revenue that meet the SBA size standard would be higher that noted herein. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[153] *See* 13 CFR § 121.201, NAICS Code 515120.

[154] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 515120, https://data.census.gov/cedsci/table?y=2017&n=515120&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[155] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[156] *See* U.S. Census Bureau, *2017 NAICS Definitions, "334290 Other Communications Equipment Manufacturing,"* https://www.census.gov/naics/?input=334290&year=2017&details=334290.

[157] *Id.*

[158] *See* 13 CFR 121.201, NAICS Code 334290.

year.[159] Of that number, 310 firms operated with fewer than 250 employees.[160] Based on this data, we conclude that the majority of Other Communications Equipment Manufacturers are small.

33. ***Fixed Microwave Services.*** Fixed microwave services include common carrier,[161] private-operational fixed,[162] and broadcast auxiliary radio services.[163] They also include the Upper Microwave Flexible Use Service (UMFUS),[164] Millimeter Wave Service (70/80/90 GHz),[165] Local Multipoint Distribution Service (LMDS),[166] the Digital Electronic Message Service (DEMS),[167] 24 GHz Service,[168] Multiple Address Systems (MAS),[169] and Multichannel Video Distribution and Data Service (MVDDS),[170] where in some bands licensees can choose between common carrier and non-common carrier status.[171] Wireless Telecommunications Carriers (*except* Satellite)[172] is the closest industry with an SBA small business size standard applicable to these services. The SBA small size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[173] U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year.[174] Of this number, 2,837 firms employed fewer than 250 employees.[175] Thus under the SBA size standard, the Commission estimates that a majority of fixed microwave service licensees can be considered small.

---

[159] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 334290, https://data.census.gov/cedsci/table?y=2017&n=334290&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[160] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[161] *See* 47 CFR part 101, subparts C and I.

[162] *See id*. subparts C and H.

[163] Auxiliary Microwave Service is governed by part 74 of Title 47 of the Commission's Rules. *See* 47 CFR part 74. Available to licensees of broadcast stations and to broadcast and cable network entities, broadcast auxiliary microwave stations are used for relaying broadcast television signals from the studio to the transmitter, or between two points such as a main studio and an auxiliary studio. The service also includes mobile TV pickups, which relay signals from a remote location back to the studio.

[164] *See* 47 CFR part 30.

[165] *See* 47 CFR part 101, subpart Q.

[166] *See id*. subpart L.

[167] *See id*. subpart G.

[168] *See id*.

[169] *See id.* subpart O.

[170] *See id*. subpart P.

[171] *See* 47 CFR §§ 101.533, 101.1017.

[172] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers* (*except Satellite*)," https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[173] *See* 13 CFR § 121.201, NAICS Code 517312.

[174] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[175] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

34. The Commission's small business size standards with respect to fixed microwave services involve eligibility for bidding credits and installment payments in the auction of licenses for the various frequency bands included in fixed microwave services. When bidding credits are adopted for the auction of licenses in fixed microwave services frequency bands, such credits may be available to several types of small businesses based average gross revenues (small, very small and entrepreneur) pursuant to the competitive bidding rules adopted in conjunction with the requirements for the auction and/or as identified in part 101 of the Commission's rules for the specific fixed microwave services frequency bands.[176]

35. In frequency bands where licenses were subject to auction, the Commission notes that as a general matter, the number of winning bidders that qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in service. Further, the Commission does not generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated. Additionally, since the Commission does not collect data on the number of employees for licensees providing these services, at this time we are not able to estimate the number of licensees with active licenses that would qualify as small under the SBA's small business size standard.

E. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

36. The Commission's part 2 rules include provisions to ensure that technical analysis and mitigation considerations underly the equipment authorization process. The Commission is authorized to dismiss or deny an application where that application is not in accordance with Commission requirements or the Commission is unable to make the finding that grant of the application would serve the public interest. The rules also require that an FCC-recognized Telecommunication Certification Body (TCB) perform "post market surveillance" of equipment that has been certified, with guidance from OET, as may be appropriate.

37. The Supplier's Declaration of Conformity (SDoC) process is available with respect to certain types of RF devices that have less potential to cause interference. The SDoC procedure requires the party responsible for compliance ("responsible party") to make the necessary measurements and complete other procedures found acceptable to the Commission to ensure that the particular equipment complies with the appropriate technical standards for that device.

38. With the adoption of this Report and Order, the Commission's rules will include specific provisions addressing the prohibition of authorizing "covered" equipment on the Covered List to help advance the Commission's goal of protecting national security and public safety from threats to the communications supply chain. The Report and Order also addresses what constitutes "covered" equipment for purposes of implementing the adopted equipment authorization prohibition. This builds on other actions the Commission recently has taken to protect and secure our nation's communications systems.

F. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

39. The RFA requires an agency to describe any significant, specifically small business, alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): "(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance or reporting requirements under the rule for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of

[176] *See* 47 CFR §§ 101.538(a)(1)-(3), 101.1112(b)-(d), 101.1319(a)(1)-(2), and 101.1429(a)(1)-(3).

the rule, or any part thereof, for such small entities."[177] In this proceeding, our adopted rule are consistent with (2), in that our goal sought comment on various steps that the Commission could take in its equipment authorization program, as well as, to reduce threats posed to our nation's communications system by "covered" equipment and services on the Covered List. We also sought comment on whether the Commission should revoke equipment authorizations of "covered" equipment, and under what conditions and procedures.

40. The Report and Order adopts several revisions to the Commission's equipment authorization program to prohibit authorization of "covered" equipment identified on the Covered List in order to protect our nation's communications systems from equipment that poses a national security risk or a threat to the safety of U.S. persons. The Report and Order regarding future authorizations of "covered" equipment are mandated by the Secure Equipment Act, requiring that the Commission "will no longer review or approve any application for equipment authorization for equipment that is on the list of covered communications equipment or services published by the Commission under section 2(a) of the [Secure Networks Act]." The equipment included on the Covered List was determined by other expert agencies as posing an unacceptable risk to national security. We find that the rules that we adopt herein involve a reasonable and cost-effective approach at this time when considering the national security concerns and the requirements of the Secure Equipment Act.

41. The Report and Order provides a revision of section 2.911 requiring that applicants for equipment authorizations in the certification process attest that their equipment is not "covered" equipment on the Covered List, coupled with procedures for revocation for false statements or misrepresentations made in the application for certification, is a reasonable and cost-effective method to ensure that "covered" equipment is not certified. Because the attestation concerns finished products, we believe that most applicants will rely on boilerplate language, that once incorporated for a single certification, will be of negligible cost for an applicant to include in future applications. We expect that our procedures for revocation for false statements or misrepresentations will deter most applicants from false attestations because of the cost that revocation would impose on an applicant. Moreover, we note that the attestation requirement that we are adopting is more cost effective than an alternative approach, such as a verification process whereby a third party would confirm that equipment being certified is not on the Covered List; that type of third party verification would be substantially more costly to applicants and would likely slow innovation. We believe that the costs we are imposing are reasonable in light of the national security goals.

42. Similarly, we find that requiring that agents for service of process on behalf of authorization grantees be located within the United States is reasonable and cost effective This will substantially reduce the cost of enforcing our prohibition on importation and marketing of equipment on the Covered List.

G. Report to Congress

43. The Commission will send a copy of the Report and Order on Protecting Against National Security Threats to the Communications Supply Chain, including this FRFA, in a report to Congress pursuant to the Congressional Review Act.[178] In addition, the Commission will send a copy of the Report and Order on Protecting Against National Security Threats to the Communications Supply Chain, including this FRFA, to the Chief Counsel for Advocacy of the SBA. A copy of the Report and Order on Protecting Against National Security Threats to the Communications Supply Chain, and FRFA (or summaries thereof) will also be published in the Federal Register.[179]

[177] 5 U.S.C. § 603(c).

[178] *See* 5 U.S.C. § 801(a)(1)(A).

[179] *See* 5 U.S.C. § 604(b).

APPENDIX C

INITIAL REGULATORY FLEXIBILITY ANALYSIS

As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] the Commission has prepared this present Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on a substantial number of small entities by the policies and rules proposed in this Further Notice of Proposed Rulemaking (Further Notice). Written public comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments in the FNPRM. The Commission will send a copy of the FNPRM, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).[2] In addition, the FNPRM and IRFA (or summaries thereof) will be published in the Federal Register.[3]

A. Need for, and Objectives of, the Proposed Rules

1. In this Further Notice, we seek further comment on proposals to protect the United States from threats to its national security through the Commission's equipment authorization program and competitive bidding process. We invite comments on additional issues related to revisions to the equipment authorization that address the Covered List,[4] component parts, revocation of equipment authorization, supply chain considerations, United States point of presence for the responsible party for certified equipment, and other issues. We also seek further comment on the risk of distortionary auction financing and potentially addressing that risk with a required auction application certification. We believe that further proposals and comment would be particularly useful for fine tuning the equipment authorization program and the competitive bidding process.

B. Legal Basis

2. The proposed action is taken under authority found in sections 4(i), 301, 302, 303, 309(j), 312, and 316 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), 301, 302a, 303, 309(j), 312 and 316, and the Secure Equipment Act of 2021, Pub. L. 117-55, 135 Stat. 423..

C. Description and Estimate of the Number of Small Entities to Which the Proposed Rules Will Apply

3. The RFA directs agencies to provide a description of, and where feasible, an estimate of the number of small entities that may be affected by the proposed rules and policies, if adopted.[5] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[6] In addition, the term "small business" has the same meaning has the term "small business concern" under the Small Business Act.[7] A "small

---

[1] 5 U.S.C. § 603. The RFA, 5 U.S.C. § 601 – 612, has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[2] 5 U.S.C. § 603(a).

[3] 5 U.S.C. § 603(a).

[4] The Covered List identifies communications equipment and services that pose an unacceptable risk to the national security of the United States or the security and safety of United States persons, pursuant to the Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601–1609) (Secure Networks Act). The Commission's Public Safety and Homeland Security Bureau maintains the list at on the Commission's website at https://www.fcc.gov/supplychain/coveredlist.

[5] 5 U.S.C. § 603(b)(3).

[6] 5 U.S.C. § 601(6).

[7] 5 U.S.C. § 601(3) (incorporating by reference the definition of "small-business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an (continued….)

business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.[8]

4. ***Small Businesses, Small Organizations, Small Governmental Jurisdictions.*** Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe, at the outset, three broad groups of small entities that could be directly affected herein.[9] First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the Small Business Administration's (SBA) Office of Advocacy, in general a small business is an independent business having fewer than 500 employees.[10] These types of small businesses represent 99.9% of all businesses in the United States, which translates to 32.5 million businesses.[11]

5. Next, the type of small entity described as a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field."[12] The Internal Revenue Service (IRS) uses a revenue benchmark of $50,000 or less to delineate its annual electronic filing requirements for small exempt organizations.[13] Nationwide, for tax year 2020, there were approximately 447,689 small exempt organizations in the U.S. reporting revenues of $50,000 or less according to the registration and tax data for exempt organizations available from the IRS.[14]

6. Finally, the small entity described as a "small governmental jurisdiction" is defined generally as "governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand."[15] U.S. Census Bureau data from the 2017 Census

---

agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register."

[8] 15 U.S.C. § 632.

[9] *See* 5 U.S.C. § 601(3)-(6).

[10] *See* SBA, Office of Advocacy, Frequently Asked Questions, "What is a small business?," https://cdn.advocacy.sba.gov/wp-content/uploads/2021/11/03093005/Small-Business-FAQ-2021.pdf. (Nov 2021).

[11] *Id*.

[12] *See* 5 U.S.C. § 601(4).

[13] The IRS benchmark is similar to the population of less than 50,000 benchmark in 5 U.S.C § 601(5) that is used to define a small governmental jurisdiction. Therefore, the IRS benchmark has been used to estimate the number small organizations in this small entity description. S*ee* Annual Electronic Filing Requirement for Small Exempt Organizations – Form 990-N (e-Postcard), "Who must file,"

https://www.irs.gov/charities-non-profits/annual-electronic-filing-requirement-for-small-exempt-organizations-form-990-n-e-postcard. We note that the IRS data does not provide information on whether a small exempt organization is independently owned and operated or dominant in its field.

[14] *See* Exempt Organizations Business Master File Extract (EO BMF), "CSV Files by Region," https://www.irs.gov/charities-non-profits/exempt-organizations-business-master-file-extract-eo-bmf. The IRS Exempt Organization Business Master File (EO BMF) Extract provides information on all registered tax-exempt/non-profit organizations. The data utilized for purposes of this description was extracted from the IRS EO BMF data for businesses for the tax year 2020 with revenue less than or equal to $50,000 for Region 1-Northeast Area (58,577), Region 2-Mid-Atlantic and Great Lakes Areas (175,272), and Region 3-Gulf Coast and Pacific Coast Areas (213,840) that includes the continental U.S., Alaska, and Hawaii. This data does not include information for Puerto Rico.

[15] *See* 5 U.S.C. § 601(5).

of Governments[16] indicate there were 90,075 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States.[17] Of this number, there were 36,931 general purpose governments (county,[18] municipal, and town or township[19]) with populations of less than 50,000 and 12,040 special purpose governments—independent school districts[20] with enrollment populations of less than 50,000.[21] Accordingly, based on the 2017 U.S. Census of Governments data, we estimate that at least 48,971 entities fall into the category of "small governmental jurisdictions."[22]

7. ***Satellite Telecommunications.*** This industry comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications."[23] Satellite telecommunications service providers include satellite and earth station operators. The SBA small business size standard for this industry classifies a business with $38.5 million or less in annual receipts as small.[24] U.S. Census Bureau data for 2017 show that 275 firms in this industry operated for the entire year.[25] Of this number, 242 firms had revenue of less than

[16] *See* 13 U.S.C. § 161. The Census of Governments survey is conducted every five (5) years compiling data for years ending with "2" and "7". *See also* Census of Governments, https://www.census.gov/programs-surveys/cog/about.html.

[17] *See* U.S. Census Bureau, 2017 Census of Governments – Organization Table 2. Local Governments by Type and State: 2017 [CG1700ORG02], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. Local governmental jurisdictions are made up of general purpose governments (county, municipal and town or township) and special purpose governments (special districts and independent school districts). *See also* tbl.2. CG1700ORG02 Table Notes Local Governments by Type and State_2017.

[18] *See id.* at tbl.5. County Governments by Population-Size Group and State: 2017 [CG1700ORG05], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 2,105 county governments with populations less than 50,000. This category does not include subcounty (municipal and township) governments.

[19] *See id.* at tbl.6. Subcounty General-Purpose Governments by Population-Size Group and State: 2017 [CG1700ORG06], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 18,729 municipal and 16,097 town and township governments with populations less than 50,000.

[20] *See id.* at tbl.10. Elementary and Secondary School Systems by Enrollment-Size Group and State: 2017 [CG1700ORG10], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 12,040 independent school districts with enrollment populations less than 50,000. *See also* tbl.4. Special-Purpose Local Governments by State Census Years 1942 to 2017 [CG1700ORG04], CG1700ORG04 Table Notes_Special Purpose Local Governments by State Census Years 1942 to 2017.

[21] While the special purpose governments category also includes local special district governments, the 2017 Census of Governments data does not provide data aggregated based on population size for the special purpose governments category. Therefore, only data from independent school districts is included in the special purpose governments category.

[22] This total is derived from the sum of the number of general purpose governments (county, municipal and town or township) with populations of less than 50,000 (36,931) and the number of special purpose governments - independent school districts with enrollment populations of less than 50,000 (12,040), from the 2017 Census of Governments - Organizations tbls.5, 6 & 10.

[23] *See* U.S. Census Bureau, *2017 NAICS Definition, "517410 Satellite Telecommunications,"* https://www.census.gov/naics/?input=517410&year=2017&details=517410.

[24] *See* 13 CFR § 121.201, NAICS Code 517410.

[25] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 517410, https://data.census.gov/cedsci/table?y=2017&n=517410&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

$25 million.[26] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 71 providers that reported they were engaged in the provision of satellite telecommunications services.[27] Of these providers, the Commission estimates that approximately 48 providers have 1,500 or fewer employees.[28] Consequently using the SBA's small business size standard, a little more than of these providers can be considered small entities.

8. ***All Other Telecommunications.*** This industry is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation.[29] This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems.[30] Providers of Internet services (e.g. dial-up ISPs) or voice over Internet protocol (VoIP) services, via client-supplied telecommunications connections are also included in this industry.[31] The SBA small business size standard for this industry classifies firms with annual receipts of $35 million or less as small.[32] U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year.[33] Of those firms, 1,039 had revenue of less than $25 million.[34] Based on this data, the Commission estimates that the majority of "All Other Telecommunications" firms can be considered small.

9. ***Fixed Satellite Transmit/Receive Earth Stations.*** There are approximately 4,303 earth station authorizations, a portion of which are Fixed Satellite Transmit/Receive Earth Stations. We do not request nor collect annual revenue information and are unable to estimate the number of the earth stations that would constitute a small business under the SBA definition. However, the majority of these stations could be impacted by our proposed rules.

10. ***Fixed Satellite Small Transmit/Receive Earth Stations***. Neither the SBA nor the Commission have developed a small business size standard specifically applicable to Fixed Satellite Small Transmit/Receive Earth Stations. Satellite Telecommunications[35] is the closest industry with an SBA small business size standard. The SBA size standard for this industry classifies a business as small

---

[26] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[27] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[28] *Id.*

[29] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517919 All Other Telecommunications,*" https://www.census.gov/naics/?input=517919&year=2017&details=517919.

[30] *Id.*

[31] *Id*.

[32] *See* 13 CFR § 121.201, NAICS Code 517919.

[33] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 517919, https://data.census.gov/cedsci/table?y=2017&n=517919&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[34] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[35] *See* U.S. Census Bureau, *2017 NAICS Definition, "517410 Satellite Telecommunications,"* https://www.census.gov/naics/?input=517410&year=2017&details=517410.

if it has $35 million or less in annual receipts.[36] For this industry, U.S. Census Bureau data for 2017 show that there were a total of 275 firms that operated for the entire year.[37] Of this total, 242 firms had revenue of less than $25 million.[38] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 71 providers that reported they were engaged in the provision of satellite telecommunications services.[39] Of these providers, the Commission estimates that approximately 48 providers have 1,500 or fewer employees.[40] Consequently using the SBA's small business size standard, a little more than half of these providers can be considered small entities.

11. ***Mobile Satellite Earth Stations.*** Neither the SBA nor the Commission have developed a small business size standard specifically applicable to Mobile Satellite Earth Stations. Satellite Telecommunications[41] is the closest industry with an SBA small business size standard. The SBA small business size standard classifies a business with $35 million or less in annual receipts as small.[42] For this industry, U.S. Census Bureau data for 2017 show that there were 275 firms that operated for the entire year.[43] Of this number, 242 firms had revenue of less than $25 million.[44] Thus, for this industry under the SBA size standard, the Commission estimates that the majority of Mobile Satellite Earth Station licensees are small entities. Additionally, based on Commission data as of December 17, 2021, there were 5 Mobile Satellite Earth Stations licensees.[45] The Commission does not request nor collect annual revenue information and is therefore unable to estimate the number of mobile satellite earth stations that would be classified as a small business under the SBA size standard.

12. ***Wireless Telecommunications Carriers (except Satellite).*** This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves.[46] Establishments in this industry have spectrum licenses and provide

---

[36] *See* 13 CFR § 121.201, NAICS Code 517410.

[37] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 517410, https://data.census.gov/cedsci/table?y=2017&n=517410&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[38] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[39] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[40] *Id.*

[41] *See* U.S. Census Bureau, *2017 NAICS Definition, "517410 Satellite Telecommunications,"* https://www.census.gov/naics/?input=517410&year=2017&details=517410.

[42] *See* 13 CFR § 121.201, NAICS Code 517410.

[43] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 517410, https://data.census.gov/cedsci/table?y=2017&n=517410&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[44] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[45] Based on a FCC International Bureau, *MyIBFS* System, Advanced Search on December 17, 2021, https://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr030b.hts?set=. Search Terms used - Nature of Application Service = SES - Satellite Earth Station; Application Type = LIC – License; Class of Station = MES – Mobile Earth Station; and under "Filing Status" = Current.

[46] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite),"* https://www.census.gov/naics/?input=517312&year=2017&details=517312.

services using that spectrum, such as cellular services, paging services, wireless internet access, and wireless video services.[47] The SBA size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[48] U.S. Census Bureau data for 2017 show that there were 2,893 firms in this industry that operated for the entire year.[49] Of that number, 2,837 firms employed fewer than 250 employees.[50] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 797 providers that reported they were engaged in the provision of wireless services.[51] Of these providers, the Commission estimates that 715 providers have 1,500 or fewer employees.[52] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities. *Wireless Carriers and Service Providers.* Wireless Telecommunications Carriers (*except* Satellite) is the closest industry with an SBA small business size standard applicable to these service providers.[53] The SBA small business size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[54] U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year.[55] Of this number, 2,837 firms employed fewer than 250 employees.[56] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 797 providers that reported they were engaged in the provision of wireless services.[57] Of these providers, the Commission estimates that 715 providers have 1,500 or fewer employees.[58] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

13. ***Wired Telecommunications Carriers.*** The U.S. Census Bureau defines this industry as establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks.[59] Transmission facilities may be based on a single technology or a

---

[47] *Id.*

[48] *See* 13 CFR § 121.201, NAICS Code 517312.

[49] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[50] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[51] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[52] *Id.*

[53] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers* (*except Satellite*)," https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[54] *See* 13 CFR § 121.201, NAICS Code 517312.

[55] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[56] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[57] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[58] *Id.*

[59] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services.[60] By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry.[61] Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.[62]

14. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[63] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[64] Of this number, 2,964 firms operated with fewer than 250 employees.[65] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 5,183 providers that reported they were engaged in the provision of fixed local services.[66] Of these providers, the Commission estimates that 4,737 providers have 1,500 or fewer employees.[67] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities. *Licenses Assigned by Auctions.* The Commission's small business size standards with respect to Licenses Assigned by Auction involve eligibility for bidding credits and installment payments in the auction of licenses for various wireless frequencies. In the auction of these licenses, the Commission may define and adopt criteria for different classes small businesses – very small, small or entrepreneur. The criteria for these small business classes may be statutorily defined in the Commission's rules[68] or may require consultation with the U.S. Small Business Administration, Office of Size Standards.[69] For licenses subject to auction, the number of winning bidders that qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in service. In addition, the Commission does not generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated.

15. *Private Land Mobile Radio Licensees*. Private land mobile radio (PLMR) systems serve an essential role in a vast range of industrial, business, land transportation, and public safety activities. Companies of all sizes operating in all U.S. business categories use these radios. Wireless

---

[60] *Id.*

[61] *Id.*

[62] Fixed Local Service Providers include the following types of providers: Incumbent Local Exchange Carriers (ILECs), Competitive Access Providers (CAPs) and Competitive Local Exchange Carriers (CLECs), Cable/Coax CLECs, Interconnected VOIP Providers, Non-Interconnected VOIP Providers, Shared-Tenant Service Providers, Audio Bridge Service Providers, and Other Local Service Providers. Local Resellers fall into another U.S. Census Bureau industry group and therefore data for these providers is not included in this industry.

[63] *See* 13 CFR § 121.201, NAICS Code 517311.

[64] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[65] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[66] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[67] *Id.*

[68] *See* 47 CFR § 27.702(a)(1)-(3). This is an illustrative example of three types of small businesses for an auction of licenses in a certain frequency that is codified in the Commission's rules.

[69] *See* 5 U.S.C. § 601(3).

Telecommunications Carriers (*except* Satellite)[70] which encompasses business entities engaged *in radiotelephone communications,* is the closest industry with an SBA small business size standard applicable to these services. The SBA small size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[71] U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year.[72] Of this number, 2,837 firms employed fewer than 250 employees.[73] Thus under the SBA size standard, the Commission estimates licensees in this industry can be considered small.

16. Based on Commission data as of December 14, 2021, there are approximately 387,370 active PLMR licenses.[74] Active PLMR licenses include 3,577 licenses in the 4.9 GHz band;[75] 19,011 licenses in the 800 MHz band;[76] and 2,716 licenses in the 900 MHz band.[77] Since the Commission does not collect data on the number of employees for licensees providing these services, at this time we are not able to estimate the number of licensees with active licenses that would qualify as small under the SBA's small business size standard. Nevertheless, the Commission believes that a substantial number of PLMR licensees are small entities.

17. ***Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing.*** This industry comprises establishments primarily engaged in manufacturing radio and television broadcast and wireless communications equipment.[78] Examples of products made by these

[70] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite),"* https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[71] *See* 13 CFR § 121.201, NAICS Code 517312.

[72] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[73] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[74] Based on a FCC Universal Licensing System search on December 14, 2021, https://wireless2.fcc.gov/UlsApp/UlsSearch/searchAdvanced.jsp. Search parameters: Service Group = All, "Match only the following radio service(s)", Radio Service = GB, GE, GF, GI, GJ, GO, GP, GU, IG, IQ, PA, PW, QM, QQ, RS, SG, SL, SP, SY, YB, YE, YF, YG, YI, YJ, YO, YP, YU, YW; Authorization Type = All; Status = Active. We note that the number of active licenses does not equate to the number of licensees. A licensee can have one or more licenses.

[75] Based on a FCC Universal Licensing System search on December 14, 2021, https://wireless2.fcc.gov/UlsApp/UlsSearch/searchAdvanced.jsp. Search parameters: Service Group = All, "Match only the following radio service(s)", Radio Service = PA; Authorization Type = All; Status = Active. We note that the number of active licenses does not equate to the number of licensees. A licensee can have one or more licenses.

[76] Based on a FCC Universal Licensing System search on December 14, 2021, https://wireless2.fcc.gov/UlsApp/UlsSearch/searchAdvanced.jsp. Search parameters: Service Group = All, "Match only the following radio service(s)", Radio Service = GB, GE, GF, GJ, GM, GO, GP, YB, YE, YF, YJ, YM, YO, YP, YX; Authorization Type = All; Status = Active. We note that the number of active licenses does not equate to the number of licensees. A licensee can have one or more licenses.

[77] Based on a FCC Universal Licensing System search on December 14, 2021, https://wireless2.fcc.gov/UlsApp/UlsSearch/searchAdvanced.jsp. Search parameters: Service Group = All, "Match only the following radio service(s)", Radio Service = GI, GR, GU, YD, YS, YU; Authorization Type = All; Status = Active. We note that the number of active licenses does not equate to the number of licensees. A licensee can have one or more licenses.

[78] *See* U.S. Census Bureau, *2017 NAICS Definition, "334220 Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing,"* https://www.census.gov/naics/?input=334220&year=2017&details=334220.

establishments are: transmitting and receiving antennas, cable television equipment, GPS equipment, pagers, cellular phones, mobile communications equipment, and radio and television studio and broadcasting equipment.[79] The SBA small business size standard for this industry classifies businesses having 1,250 employees or less as small.[80] U.S. Census Bureau data for 2017 show that there were 656 firms in this industry that operated for the entire year.[81] Of this number, 624 firms had fewer than 250 employees.[82] Thus, under the SBA size standard, the majority of firms in this industry can be considered small.

18. ***Auxiliary, Special Broadcast and Other Program Distribution Services.*** This service involves a variety of transmitters, generally used to relay broadcast programming to the public (through translator and booster stations) or within the program distribution chain (from a remote news gathering unit back to the station). Neither the SBA nor the Commission have developed a small business size standard applicable to broadcast auxiliary licensees. The closest applicable industries with an SBA small business size standard fall within two industries - Radio Stations[83] and Television Broadcasting.[84] The SBA small business size standard for Radio Stations classifies firms having $41.5 million or less in annual receipts as small.[85] U.S. Census Bureau data for 2017 show that 2,963 firms operated in this industry during that year.[86] Of that number, 1,879 firms operated with revenue of less than $25 million per year.[87] For Television Broadcasting, the SBA small business size standard also classifies firms having $41.5 million or less in annual receipts as small.[88] U.S. Census Bureau data for 2017 show that 744 firms in this industry operated for the entire year.[89] Of that number, 657 firms had revenue of less

[79] *Id*.

[80] *See* 13 CFR § 121.201, NAICS Code 334220.

[81] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 334220, https://data.census.gov/cedsci/table?y=2017&n=334220&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[82] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[83] *See* U.S. Census Bureau, *2017 NAICS Definition, "515112 Radio Stations*," https://www.census.gov/naics/?input=515112&year=2017&details=515112.

[84] *See* U.S. Census Bureau, *2017 NAICS Definition, "515120 Television Broadcasting,*" https://www.census.gov/naics/?input=515120&year=2017&details=515120.

[85] *See* 13 CFR § 121.201, NAICS Code 515112.

[86] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 515112, https://data.census.gov/cedsci/table?y=2017&n=515112&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false. We note that the US Census Bureau withheld publication of the number of firms that operated for the entire year.

[87] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We note that the U.S. Census Bureau withheld publication of the number of firms that operated with sales/value of shipments/revenue in the individual categories for less than $100,000, and $100,000 to $249,999 to avoid disclosing data for individual companies (see Cell Notes for the sales/value of shipments/revenue in these categories). Therefore, the number of firms with revenue that meet the SBA size standard would be higher that noted herein. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[88] *See* 13 CFR § 121.201, NAICS Code 515120.

[89] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 515120, https://data.census.gov/cedsci/table?y=2017&n=515120&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

than $25 million per year.[90] Accordingly, based on the U.S. Census Bureau data for Radio Stations and Television Broadcasting, the Commission estimates that the majority of Auxiliary, Special Broadcast and Other Program Distribution Services firms are small under the SBA size standard.

19. ***Radio Frequency Equipment Manufacturers (RF Manufacturers).*** There are several analogous industries with an SBA small business size standard that are applicable to RF Manufacturers. These industries are Fixed Microwave Services, Other Communications Equipment Manufacturing, and Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing. A description of these industries and the SBA small business size standards are detailed below.

20. ***Fixed Microwave Services.*** Fixed microwave services include common carrier,[91] private-operational fixed,[92] and broadcast auxiliary radio services.[93] They also include the Upper Microwave Flexible Use Service (UMFUS),[94] Millimeter Wave Service (70/80/90 GHz),[95] Local Multipoint Distribution Service (LMDS),[96] the Digital Electronic Message Service (DEMS),[97] 24 GHz Service,[98] Multiple Address Systems (MAS),[99] and Multichannel Video Distribution and Data Service (MVDDS),[100] where in some bands licensees can choose between common carrier and non-common carrier status.[101] Wireless Telecommunications Carriers (*except* Satellite)[102] is the closest industry with an SBA small business size standard applicable to these services. The SBA small size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[103] U.S. Census Bureau data for 2017 show that there were 2,893 firms that operated in this industry for the entire year.[104] Of this number,

[90] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[91] *See* 47 CFR part 101, subparts C and I.

[92] *See id*. subparts C and H.

[93] Auxiliary Microwave Service is governed by part 74 of Title 47 of the Commission's Rules. *See* 47 CFR part 74. Available to licensees of broadcast stations and to broadcast and cable network entities, broadcast auxiliary microwave stations are used for relaying broadcast television signals from the studio to the transmitter, or between two points such as a main studio and an auxiliary studio. The service also includes mobile TV pickups, which relay signals from a remote location back to the studio.

[94] *See* 47 CFR part 30.

[95] *See* 47 CFR part 101, subpart Q.

[96] *See id*. subpart L.

[97] *See id*. subpart G.

[98] *See id*.

[99] *See id.* subpart O.

[100] *See id*. subpart P.

[101] *See* 47 CFR §§ 101.533, 101.1017.

[102] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers* (*except Satellite*)," https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[103] *See* 13 CFR § 121.201, NAICS Code 517312.

[104] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

2,837 firms employed fewer than 250 employees.[105] Thus under the SBA size standard, the Commission estimates that a majority of fixed microwave service licensees can be considered small.

21. The Commission's small business size standards with respect to fixed microwave services involve eligibility for bidding credits and installment payments in the auction of licenses for the various frequency bands included in fixed microwave services. When bidding credits are adopted for the auction of licenses in fixed microwave services frequency bands, such credits may be available to several types of small businesses based average gross revenues (small, very small and entrepreneur) pursuant to the competitive bidding rules adopted in conjunction with the requirements for the auction and/or as identified in part 101 of the Commission's rules for the specific fixed microwave services frequency bands.[106]

22. In frequency bands where licenses were subject to auction, the Commission notes that as a general matter, the number of winning bidders that qualify as small businesses at the close of an auction does not necessarily represent the number of small businesses currently in service. Further, the Commission does not generally track subsequent business size unless, in the context of assignments or transfers, unjust enrichment issues are implicated. Additionally, since the Commission does not collect data on the number of employees for licensees providing these services, at this time we are not able to estimate the number of licensees with active licenses that would qualify as small under the SBA's small business size standard.

23. ***Other Communications Equipment Manufacturing.*** This industry comprises establishments primarily engaged in manufacturing communications equipment (except telephone apparatus, and radio and television broadcast, and wireless communications equipment).[107] Examples of such manufacturing include fire detection and alarm systems manufacturing, Intercom systems and equipment manufacturing, and signals (e.g., highway, pedestrian, railway, traffic) manufacturing.[108] The SBA small business size standard for this industry classifies firms having 750 or fewer employees as small.[109] For this industry, U.S. Census Bureau data for 2017 shows that 321 firms operated for the entire year.[110] Of that number, 310 firms operated with fewer than 250 employees.[111] Based on this data, we conclude that the majority of Other Communications Equipment Manufacturers are small.

24. ***Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing.*** This industry comprises establishments primarily engaged in manufacturing radio and television broadcast and wireless communications equipment.[112] Examples of products made by these establishments are: transmitting and receiving antennas, cable television equipment, GPS equipment,

---

[105] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[106] *See* 47 CFR §§ 101.538(a)(1)-(3), 101.1112(b)-(d), 101.1319(a)(1)-(2), and 101.1429(a)(1)-(3).

[107] *See* U.S. Census Bureau, *2017 NAICS Definitions, "334290 Other Communications Equipment Manufacturing,"* https://www.census.gov/naics/?input=334290&year=2017&details=334290.

[108] *Id.*

[109] *See* 13 CFR 121.201, NAICS Code 334290.

[110] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 334290, https://data.census.gov/cedsci/table?y=2017&n=334290&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[111] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[112] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*334220 Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing,*" https://www.census.gov/naics/?input=334220&year=2017&details=334220.

pagers, cellular phones, mobile communications equipment, and radio and television studio and broadcasting equipment.[113] The SBA small business size standard for this industry classifies firms having 1,250 employees or less as small.[114] U.S. Census Bureau data for 2017 show that there were 656 firms in this industry that operated for the entire year.[115] Of this number, 624 had fewer than 250 employees.[116] Based on this data, we conclude that a majority of manufacturers in this industry are small.

D. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

25. Under the proposals set forth in the Further Notice, and consistent with the Commission's general approach, we expect that all the filing, recordkeeping and reporting requirements associated with the proposed rules would be the same for large and small businesses; however, we seek comment on any steps that could be taken to minimize any significant economic impact on small businesses. The proposals being made in this Further Notice may require additional provisions in the part 2 rules to help ensure the integrity of the equipment authorization process. In this Further Notice, we examine our part 2 and 15 rules relating to equipment authorization and participation in Commission auctions to help advance the Commission's goal of protecting national security and public safety. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

E. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

26. The RFA requires an agency to describe any significant, specifically small business, alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): "(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance or reporting requirements under the rule for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities."[117] In this proceeding, our proposals are consistent with (2) and (4), in that our goal is to seek comment on various steps that the Commission could take in its equipment authorization program, as well as its competitive bidding program, to reduce threats posed to our nation's communications system by "covered" equipment and services on the Covered List. We also seek comment on whether the Commission should revoke equipment authorizations of "covered" equipment, and if so under what conditions, procedures and how it will apply.

27. The Further Notice seeks additional comment on requiring that the responsible party of authorized equipment be located in the United States. The currently-effective comparable rules associated with the Supplier's Declaration of Conformity (SDoC) are narrowly tailored and a cost-effective means of achieving the Commission's national security goals in this proceeding.

28. In order to effectively use our equipment authorization program to protect against equipment with security concerns, we seek further comment on how to subject all "covered" equipment to prohibition under our part 2 equipment authorization rules and what amendments are necessary to the part 15 rules that otherwise provide unlicensed equipment an exemption from equipment authorization

---

[113] *Id.*

[114] *See* 13 CFR § 121.201, NAICS Code 334220.

[115] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 334220, https://data.census.gov/cedsci/table?y=2017&n=334220&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[116] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[117] 5 U.S.C. § 603(c).

requirements. We believe rule amendments that apply to all part 15 equipment would be a cost-effective means of achieving the Commission's goals, and certainly less costly than a registry or attestation systems for otherwise exempt equipment produced by any of the entities who have "covered" equipment on the Covered List.

F. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules

29. None.

APPENDIX D

List of Commenters

5G Americas

Alpha Prime Communications

The App Association

Baker's Communications

Jordan A. Brunner

Charter Communications, Inc.

China Tech Threat and BluePath Labs

Chown Hardware

Coalition for a Prosperous America

Communications Associates

Computer Supporter & Associates

Consumer Technology Association

CTIA

Dahua Technology USA, Inc.

Diversified Communications Group

DroneDeploy

Eagle Communications

East Mountain Communications

Eastern CCTV USA LLC d.b.a. ENS Security

ACT – The App Association; Consumer Technology Association; Council to Secure the Digital Economy; CTIA; Internet Association; Information Technology Industry Council; Telecommunications Industry Association; and US Telecom

FreCom, Inc.

GCS Electronics & Communications

Gen Net, Inc.

Hikvision USA Inc.

Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc.

Hytera Communications Corporation Limited

Hytera US

Information Technology Industry Council

Intertek

IPVM

Clete D. Johnson and Jennifer B. Tatel

Jack Corrigan/Center for Security and Emerging Technology
JVCKenwood USA Corporation
Don Kwapien
Metrotalk
Minnesota Telephone Networks
Mobile and Wireless Forum
Motorola Solutions, Inc.
NCTA – The Internet and Television Association
New Jersey Transit Corporation
NTCA – The Rural Broadband Association
Panasonic i-PRO Sensing Solutions Corporation
PowerTrunk, Inc.
People's Republic of China
RadioMax Communications Inc.
Darcie Reichert
Rear Adm. (ret.) David G. Simpson
S-Tech Solutions
Telecommunications Industry Association
Shane Tews
U.S. Chamber of Commerce
US Telecom – The Broadband Association
Noah Vehafric
Voceon Digital Radio Communications
Warner Communications
Aaron Oakley
Aaron Shaner
Advanced Business Communications Inc
Allan Peda
Allegiant Security Cameras LLC
Andrew Harvey
Andrew J. Staves
Andy Crane
Angel Cruz Martinez
Anthony DeStefano
Art Verling
Automated Lifestyles LLC

Barrier Protection Systems Inc, Kasey Kennedy

Ben Brooks

Ben Kiser

Billy Marsh

Bob Ray

Brian Hodge

Brian Stowers

Bruce Marcus

Bryan Parrott

Charles Vowell

Chris Hill

Chris Lohr

Chris Parker

Christopher Danzberger

Ciprian Pasare

Craig A. Waltzer

CRB Security Solutions

Curtis Maglinger

Dahua Technology USA Inc

Dan Uelman

Daniel Baran

Daniel J Lopez

Danny Chang

Darryl Mendivil

Darwin Roach

Darwin Smith

Dave Kotler, Jody Kotler, Tony Albenese

David Garrett

David Howard

David Pilchick

David Suarez

Domenic LaRocca

Don Richter

Douglas Scot Browning

ECS, Access Group Inc, Scott Evans

Ed Grantier

Electronics Supply Co., Inc.
Emilie Salsitz
Eric Medecke
Faisal Farooqui
Frank Fritz, Intellitech Systems, Inc
Gary Mikaelian
Glenn Security Systems, Inc.
Halo Technologies & Security
Heather Martin
Holli Fadem
Israel Thaler
James M Starr
James Sielaff
Jared Wilson
Jason Buchanan
Jason Walsh, Marian Bassalious
Jeff Altenbernd
Jeff Massey
Jeff Sly
Jennifer Kern
Jerry De Francisco
Joe Polizzi
John Minasyan
John Prindle
John Taylor
John Yeung
Jon Harden
Joseph Crossley
Josh Geddings
Juda Slomovich
Kevin Bradley
Kevin Dutton
KOA Electronics Distribution Inc.
Kugugibi
Kyle Folger
Lloyd Hall

Mario Ramos
Mark Crumbacher
Mark McGinnis
Mark Nardontonia
Mark Zuckerman
Martin Paikin
Martin VanConant
Mason Shelby
Matt Smith
Matthew Daughtry
Matthew Duffy
Maxtech Security Systems Inc.
Mayer Sprecher
Michael Bolton
Michael Cassettari, ACP Communications Corp
Michael Edwards
Michael Maslowski
Michael Milhauser
Michael Pikman
Michael Pittman
Michael Proudfit Titan Alarm Inc.
Michael Young
MicroMagic Radio Communications
Mike Hall
Mike Markham
Mike McDonald
Mike Taylor
MyrtleNET
Neal Niswender
Nelya Galiy
Odyssey Technologies, Inc.
Oscar Cortes
Parker Ledbetter
Patrick T Presto - M&P Security Solutions LLC
Paul Bockert
Philip Todd

Randy Elrod

Ray Johnson, Appliedtelecomanddata.com

Raymond K. Shadman

R. D. Stephenson

Richard Rizzo

Rob Waitman

Robert Shields

Robert Wolff

Ron D. Eliseo

Ron Valdez

Ronald W. Best

Roy Stella

Russell Chernak

Sam Jazaerli

Sargon Younan

Scott Joyce

Scott T Shaw

Sean Hamm

Sean Nelson

Shahe Bezdjian

Shane Nevins

Sheppard Security & Communication Inc., James W. Sheppard Jr., Galen Keith Sheppard

Steve Kaufer

Steve Lawrence

Steve McGuire

Stu Forchheimer

Surlonda

T and J Communications DBA - TELCOMTEC INC.

Taylor Proudfit

Tewa Canterbury

The Alarm Guy Security

The Edge Group

Timothy Hinson

Timothy L. Smith

Troy Duncan, JUNTO Technology, LLC.

Uriah Ortiz, Sylvia Ortiz

William Bew

Yisrael Gold

STATEMENT OF
CHAIRWOMAN JESSICA ROSENWORCEL

Re: *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*; *Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program*, ET Docket No. 21-232, EA Docket No. 21-233, Report and Order, Order, and Further Notice of Proposed Rulemaking

Communications networks are a part of everything we do. We use them to connect with family and friends. We use them to build commercial businesses and civil society. We use them for healthcare and education. We use them to make purchases, seek out news, and get the facts we need to make decisions about our lives, our communities, and our country.

It's a lot and it's why the security of our communications networks matters more than ever before. Yet the truth is we are just getting started. Because in the not-too-distant future these networks will expand to connect everything around us. They will open up possibilities for communications and computing that we cannot even fully imagine today. By exponentially increasing the connections between people and things, communications technologies could become an input in everything we do—improving agriculture, education, healthcare, energy, transportation, and more. The data we will derive from all these connections will be powerful and will inform the next generation of innovation across the economy.

It is essential that we plan for this future right now. That's because we need to ensure the networks we know today become more secure over time and evolve to withstand cyberattack from those who wish to do us harm. After all, with insecure networks it is too easy for bad actors to introduce viruses and malware, steal private data, engage in intellectual property theft, and surveil companies and government agencies.

That is why at the Federal Communications Commission we have made network security a top priority—and we have a long list of accomplishments to show for it.

For starters, we have taken action to improve awareness about network vulnerabilities, threats, and breaches within the federal government and the private sector. On March 12, 2021, we published the first-ever list of communications and services that pose an unacceptable risk to national security as required under the Secure and Trusted Communications Networks Act. This initial Covered List included equipment from the Chinese companies Huawei, ZTE, Hytera, Hikvision, and Dahua. Since then, we've added equipment and services from five additional entities. Last year I also proposed stricter data breach reporting rules and worked with the Department of State to improve how we coordinate national security issues related to submarine cable licenses.

Next, we took concrete action to defend against the threats and vulnerabilities that were identified through our work. We launched the Secure and Trusted Communications Networks Reimbursement Program to remove untrusted equipment from our networks and replace them with secure alternatives. Working with our national security colleagues, we revoked the section 214 operating authorities of four Chinese state-owned carriers who were providing service in the United States. Last month, we required Emergency Alert System and Wireless Emergency Alert System participants to have a cybersecurity risk management plan in place. We also announced a first-of-its-kind settlement against a company that will require it to divest unvetted Russian ownership, pay a civil penalty, and put in place new security procedures to review any new ownership through the Office of Foreign Asset Control at the Treasury Department.

Finally, we took steps to build security into what comes next. We launched new inquiries on the security of internet routing and the Internet of Things. I recharted the Communications Security, Reliability, and Interoperability Council and, for the first time, designated the Cybersecurity and Infrastructure Security Agency as co-chair. And I revitalized the Cybersecurity Forum for Independent and Executive Branch Regulators to share information and expertise and enhance the cybersecurity of the nation's critical infrastructure.

Together, these efforts will make our networks more secure. But today we go a step further, by addressing not just communications but the process we use to authorize communications equipment in the United States.

Let me explain. While we've flagged equipment as posing a national security risk, prohibited companies from using federal funds to purchase them, and even stood up programs to replace them, for the last several years the FCC has continued to put its stamp of approval on this equipment through its equipment authorization process. So long as this equipment carries that stamp, it can continue to be imported into the United States and sold to buyers who are not using federal funds.

But that does not make any sense. After all, there is little benefit in having these lists and these bans in place just to leave open other opportunities for this equipment to be present in our networks. So today we are taking action to align our equipment authorization procedures with the rest of our national security policies.

Specifically, under the rules we adopt today pursuant to the Secure Equipment Act, the FCC will no longer authorize equipment that is on the Covered List because it poses an unacceptable risk to the national security of the United States or the safety of United States persons. That includes telecommunications and video surveillance equipment from Huawei and ZTE. It also includes telecommunications and video surveillance equipment from Hytera, Hikvision, and Dahua that is used for the purpose of public safety, security of government facilities, physical surveillance of critical infrastructure, and other national security purposes. For these three companies, we will require them to document what safeguards they will put in place on marketing or sale for these purposes and we are putting in place a freeze on all of their telecommunications and video surveillance equipment authorization applications until that work is done.

The action we take today covers base station equipment that goes into our networks. It covers phones, cameras, and Wi-Fi routers that go into our homes. And it covers re-branded or "white label" equipment that is developed for the marketplace. In other words, this approach is comprehensive.

However, because we recognize that these issues may evolve over time, we also adopt a further rulemaking to invite additional comment on the need to update our equipment approval process to address component parts. We also ask how and if it is necessary to consider the revocation of any existing authorization for covered equipment in the future.

This order and rulemaking is part of our broader focus on network security and I am grateful for the support of my colleagues Commissioner Carr, Commissioner Starks, and Commissioner Simington in this effort. I also want thank the Congressional champions of the Secure Equipment Act, including Senator Markey, Senator Rubio, Congresswoman Eshoo, and Congressman Steve Scalise, for their support for the work of this agency and laser-like focus on the steps we can take to address insecure communications and network equipment.

STATEMENT OF
COMMISSIONER BRENDAN CARR

Re: *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*; *Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program*, ET Docket No. 21-232, EA Docket No. 21-233, Report and Order, Order, and Further Notice of Proposed Rulemaking

Today, the FCC takes an unprecedented step to safeguard our communications networks and strengthen America's national security. Our unanimous decision represents the first time in the FCC's history that we have voted to prohibit the authorization of communications and electronic equipment based on national security considerations. And we take this action with the broad, bipartisan backing of congressional leadership.

In March of 2021, in remarks at the Center for Strategic and International Studies (CSIS), I called for the FCC to take this action as a necessary step in our ongoing efforts to address the threats posed by Communist China and other malign actors—entities that would be all too eager to exploit backdoors in our electronics systems to obtain sensitive information and exploit that access to endanger America's interests through espionage, IP theft, blackmail, foreign influence campaigns, and other nefarious activities. At the time, I noted that the FCC's then-unprecedented decision in 2020 to prohibit the use of federal universal service subsidies to purchase equipment from companies like Huawei that pose an unacceptable national security threat represented real progress towards safeguarding our networks. Indeed, many carriers that would have otherwise purchased Huawei gear ceased doing so as a result of the FCC's 2020 rules. But as I pointed out during the CSIS remarks, those FCC rules expressly allowed carriers to use private funds to purchase the exact same equipment and place it in the exact same point in their networks. I argued that it was time to close this Huawei loophole. I am thankful that we do exactly that today.

After all, once we have determined that equipment from certain manufacturers poses an unacceptable national security risk, it makes no sense to allow that exact same equipment to be purchased and inserted into our communications networks as long as federal dollars are not involved. It is the presence of this insecure gear in our networks that presents the threat—not the source of funding used to purchase it. Yet the FCC, through its equipment authorization process, had been continuing to approve for use in the U.S. literally thousands of new applications from Huawei and other bad actors. As I noted, there is virtually no piece of electronics or communications equipment that can be used in the U.S. without an approval issued by the FCC through its equipment authorization process. So I called on the FCC to use its existing authority to deny equipment authorizations to any entity that is on the Commission's Covered List—a move that would get at the problem root and branch. Today, the FCC's Covered List includes equipment from Huawei, ZTE, Hytera, Hikvision, and Dahua.

Notably, the FCC's proposal to deny equipment authorizations involving insecure equipment garnered broad and bipartisan support. Indeed, Congress enacted and President Biden signed the Secure Equipment Act into law in November 2021 directing the FCC to complete this proceeding and in doing so provided the FCC with an additional set of authorities to act.

I also want to thank my FCC colleagues for agreeing to bolster our decision today. For instance, we now decide in this Order that the FCC has the authority to revoke existing equipment authorizations. This is an important determination, and while this Order does not take the step of revoking any equipment authorizations—focusing instead on the very important action of prohibiting the approval of new

applications for covered equipment consistent with language that Congress included in the Secure Equipment Act—I am gratified that the agency has now put revocations squarely on the table. I hope that we soon exercise that authority, and I look forward to working with my colleagues on achieving that end.

Today's decision is not a final step in our work to secure America's communication networks. Far from it. I have identified a number of additional, concrete steps we should take to protect consumers. In addition, one near term action that I recommend is for the Commission to work with the national security agencies to expand the scope of equipment from Hikvision, Dahua, and Hytera—entities with deep ties to Communist China's surveillance operation—that should be included on our Covered List. This would further strengthen our equipment authorization actions and allow us to prohibit the use of Hikvision, Dahua, and Hytera equipment in an even broader set of circumstances. We must also vigilantly monitor compliance with the rules we've established today, including by ensuring that entities do not make an end run around our decision by "white labeling" covered gear—a process that involves putting a benign or front group's name on equipment that would otherwise be subject to our prohibitions. And of course, secure networks mean little if insecure applications are allowed to run, sweep up much of the same sensitive data, and send it back to Beijing. So I would encourage the Treasury Department and the FCC's sister agencies to reach a final decision in their ongoing reviews of TikTok.

In closing, I want to offer my sincere thanks and appreciation to the many people whose hard work and leadership got us here today. To start, Chairwoman Rosenworcel deserves much credit for her longstanding commitment to protecting consumers and ensuring the Commission is engaging through the appropriate channels on national security issues. Similarly, Commissioner Starks and Commissioner Simington are champions for network security and have my appreciation for our continued partnership. Additionally, the momentum and support provided by Congress has greatly helped our ability to reach our decision today. For that, Senator Rubio, Senator Markey, Republican Whip Scalise, and Congresswoman Eshoo deserve heaps of credit. And last but of course not least, many thanks to the hardworking and talented Commission staff across the Office of Engineering and Technology, the Office of Public Safety and Homeland Security Bureau, the Office of General Counsel, the Wireline Competition Bureau, the Office of Economics and Analytics, the Enforcement Bureau, the International Bureau, and the Wireless Telecommunications Bureau who worked tirelessly on today's item.

STATEMENT OF
COMMISSIONER GEOFFREY STARKS

Re: *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*; *Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program*, ET Docket No. 21-232, EA Docket No. 21-233, Report and Order, Order, and Further Notice of Proposed Rulemaking

In 2019, I called for the Commission to examine its equipment authorization authority as a possible tool for improving our network security. Three years later, I'm very glad to support the Commission's action in this item. By stopping equipment identified as a threat to the United States from entering our markets, we significantly decrease the risk that it can be used against us. We also lower the possibility that we'll need to rip and replace that equipment in the future. Ultimately, if it can't get authorized, it can't be deployed.

The item is a thorough effort to secure our equipment authorization process. It amends the authorization rules to close loopholes and increases our ability to enforce our rules when a violation does occur. I want to highlight three specific policy decisions that will make a big difference in mitigating risk from untrusted and insecure equipment going forward.

First, I support amending our equipment authorization program to eliminate potential loopholes whereby equipment that is listed on our List of Covered Communications Equipment and Services (Covered List)[1] could still be authorized and allowed to enter into the United States. Specifically, by closing the possibility of using the Supplier Declaration of Conformity process if an entity produces covered equipment, we shift oversight of these higher risk entities to the certification process. This will make sure that equipment receiving authorization is clearly eligible.

Second, as a former enforcement official, I strongly support strengthening enforcement of our rules by requiring that each applicant for equipment certification designate a contact located in the United States for purposes of acting as its agent for service of process, regardless of whether the applicant is a domestic or foreign entity. When I originally proposed that the Notice do just this, it was an effort to eliminate the loophole that too many bad actors had used to evade enforcement of our rules in the past.[2] No more. If you want to be authorized to sell your equipment in the United States, we must be able to enforce our rules against you if you violate them. Full stop.

Third, the Report and Order properly eliminates equipment authorization for "white labeled equipment." White labeled equipment is equipment produced by one company that is marketed or branded under another's name. Re-branding insecure equipment does nothing to change the threat profile. In fact, it can increase risk because consumers may be more trusting of one brand than they otherwise would be if they knew who actually made it. I support the decision to close this gap that could render our new equipment authorization prohibitions less effective.

Additionally, the Further Notice seeks comment on a number of important issues. It is important that we continue to develop the record on revocation of existing equipment authorizations and a potential requirement regarding a point of presence for enforcement purposes. But, I want to focus on the

[1] The Covered List is available on the FCC's website at https://www.fcc.gov/supplychain/coveredlist.

[2] *Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program*, EA Docket No. 21-233, Notice of Proposed Rulemaking and Notice of Inquiry, 36 FCC Rcd 10578, Statement of Commissioner Geoffrey Starks at 1 (2021).

importance of building a record regarding how our equipment authorization should handle components made by entities identified on the Covered List.

As the record shows, components of equipment deemed to pose a threat to the United States can pose the same risk as equipment itself. This is especially the case for advanced components or electrical components—those which can process and/or retain data. When the Commission created the Reimbursement Program, it identified the risk that certain components of Huawei and ZTE equipment could pose if—after being removed from our communications networks—those components somehow made their way back into equipment deployed in telecommunications networks. We required that both the equipment—and the components that could process and/or retain data—be destroyed,[3] consistent with Congress' direction that equipment that is removed and replaced also be destroyed.[4]

So, I'm glad my colleagues agreed to my edits to add additional questions about how the Commission should consider components of equipment listed on the Covered List. I also appreciate their support of my edits to include questions about efforts elsewhere in the United States government working on similar challenges. Specifically, we should coordinate with our fellow agencies on a whole-of-government approach with regard to components. Several agencies are working on similar efforts, such as the Hardware Bill of Materials and the Software Bill of Materials.[5] We should consider coordinating and taking advantage of the work already done by those agencies, and groups such as the Information and Communications Technology Supply Chain Risk Management Task Force,[6] to inform our actions going forward.

I thank Chairwoman Rosenworcel and my fellow Commissioners for working with me to improve the item, and for their leadership in working together to protect our nation and networks from equipment deemed to pose a threat. I thank the fantastic FCC staff, especially those in the Office of Engineering and Technology, Public Safety and Homeland Security Bureau, the Office of General Counsel, the International Bureau, the Wireless Telecommunications Bureau, the Enforcement Bureau, the Wireline Competition Bureau, and the Office of Economics and Analytics for their hard work on this challenging proceeding. This item has my strong support.

---

[3] *Wireline Competition Bureau Announces Best Practices for Equipment Disposal and Revises FCC Form 5640 Certifications for the Secure and Trusted Communications Networks Reimbursement Program*, WC Docket No. 18-89, Public Notice, DA 21-1234, at 14064 (Sept. 30, 2021).

[4] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1603(d)(7). *See also* H.R. Rep. No. 116-352, at 14 (2019) ("Any applicant receiving reimbursement funds under the Program is required to complete the permanent removal, replacement, and disposal of covered equipment and services from their networks not later than one year after the date on which the Commission distributes funds to the applicant.").

[5] Software Bill of Materials, Cybersecurity and Infrastructure Security Agency, *available at* https://www.cisa.gov/sbom (last visited Nov. 22, 2022).

[6] ICT Supply Chain Risk Management Task Force, Cybersecurity and Infrastructure Security Agency, *available at* https://www.cisa.gov/ict-scrm-task-force (last visited Nov. 22, 2022).

STATEMENT OF
COMMISSIONER NATHAN SIMINGTON

Re: *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*; *Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program*, ET Docket No. 21-232, EA Docket No. 21-233, Report and Order, Order, and Further Notice of Proposed Rulemaking

I'm proud to vote to approve the implementation of the Secure Equipment Act, banning untrustworthy equipment from our country's networks. This is the culmination of a bipartisan effort spanning multiple presidential and FCC administrations, and it will help make Americans more secure by preventing hostile governments from using their technology exports to establish footholds in our networks.

I want to thank the FCC staff for their especially hard work on this item. The Secure Equipment Act is a complex law, and they succeeded in the challenging task of turning it into an effective regulatory scheme. They should be proud.

But as we celebrate this victory, we cannot forget that our work to secure our country from insecure and untrustworthy equipment is only just beginning. In addition to banning equipment from untrustworthy state-controlled companies, as we have done here, we need to address the proliferation of insecure devices more generally. Hundreds of millions of actively used wireless devices in our country are susceptible to security vulnerabilities for which they will never be patched. This is a ticking time bomb for the security of our wireless networks and devices, and a disincentive to building more, because the public will have justified, low expectations of their security.

We all know the risks of attackers gaining access to sensitive consumer, business, and government data and controls through insecure wireless devices. But we also need to think about distributed signal jamming attacks and the other new vulnerabilities that wireless technologies expose for spoofing, sniffing, and jamming attacks. If we are to fulfill our mission to increase the adoption of sophisticated communications services while managing the use of spectrum to the public benefit, we must ensure that the public can have total confidence in signal security. I hope the FCC takes strong action to defend against these threats and to anticipate them before they manifest as crises.

PROOF OF SERVICE

I, Matthew J. Dunne, hereby certify that on February 27, 2023, a copy of the foregoing NOTICE TO THE UNITED STATES JUDICIAL PANEL ON MULTIDISTRICT LITIGATION OF MULTICIRCUIT PETITIONS FOR REVIEW was served by using the electronic CM/ECF system to the following courts:

Clerks of Court

Molly Dwyer, Clerk of Court Office of the Clerk U.S. Court of Appeals for the Ninth Circuit P.O. Box 193939 San Francisco, CA 94119-3939 (415) 355-8000 www.ca9.uscourts.gov	Mark Langer, Clerk of Court Office of the Clerk U.S. Court of Appeals for the District of Columbia Circuit Room 5205 E. Barret Prettyman U.S. Courthouse and William B. Bryant Annex 333 Constitution Ave., NW Washington, DC 20001 (202) 216-7000

Copies of the foregoing Notice were also sent by using the electronic CM/ECF system to following counsel:

John T. Nakahata Christopher J. Wright Timothy J. Simeone John R. Grimm Deepika Ravi HWG, LLP 1919 M. St., NW, 8th Floor Washington, DC 20036 (202) 730-1300 jnakahata@hwglaw.com cwright@hwglaw.com tsimeone@hwglaw.com jgrimm@hwglaw.com dravi@hwglaw.com *Counsel for: Hikvision USA, Inc.*	Andrew D. Lipman Russell M. Blau MORGAN, LEWIS & BOCKIUS LLP 1111 Pennsylvania Avenue, NW Washington, DC 20004 (202) 739-3000 andrew.lipman@morganlewis.com russell.blau@morganlewis.com *Counsel for: Dahua Technology USA Inc.*

/s/ Matthew J. Dunne

Matthew J. Dunne
Counsel

Federal Communications Commission
Washington, DC 20554
(202) 418-1740
matthew.dunne@fcc.gov
fcclitigation@fcc.gov